LOPD: OBLIGACIONES DE TODOS LOS USUARIOS QUE TRATEN CON DATOS PERSONALES (versión 1.1, fecha 19/02/2014)

La LOPD (Ley Orgánica de Protección de Datos de carácter personal) tiene como objetivo garantizar y proteger los derechos fundamentales de las personas físicas y, especialmente, su honor e intimidad personal y familiar.

Por eso, esta ley obliga a BARBERÁN y a todos sus empleados y profesionales con acceso a datos personales a proteger la información almacenada en sus sistemas informáticos y archivos documentales. (Se considera dato personal cualquier dato sobre personas físicas, incluyendo por tanto los datos de los propios empleados, las personas de contacto o nombres de clientes y proveedores, etc.)

BARBERÁN, en cumplimiento de la LOPD, ha registrado en la Agencia Española de Protección de Datos los ficheros existentes con datos personales (tanto en nuestro sistema informático, como en nuestros archivos documentales), aplica todas las obligaciones legales que establece la ley, como la inclusión de los avisos legales en la recogida de los datos, y dispone de un documento de seguridad que especifica las medidas técnicas, jurídicas y organizativas necesarias para cumplir con la legislación vigente que se aplican.

Por su parte, todos los usuarios de datos de carácter personal, tanto almacenados en sistemas informáticos como en papel, deben cumplir las siguientes normas encaminadas a asegurar un buen cumplimiento de la LOPD, así como de alguna otra ley relacionada (LSSI o Ley de Servicios de la Sociedad de la Información y de comercio electrónico; LGT o Ley General de Telecomunicaciones)

1) Deber de secreto

El usuario está obligado al secreto profesional respecto a los datos de carácter personal y al deber de guardarlos y no difundirlos, obligación que subsistirá aun después de finalizar sus relaciones con BARBERÁN.

2) Puestos de trabajo

El usuario es responsable del puesto de trabajo desde donde realiza el acceso, y garantizará que ninguna otra persona no autorizada pueda ver la información sobre datos personales que muestran sus equipos informáticos. Es decir que, tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad. Cuando el usuario abandone el puesto de trabajo, ya sea temporalmente o por terminar su jornada laboral, el usuario, como responsable del mismo, deberá dejar los sistemas informáticos de manera que sea imposible la visualización de los datos protegidos. Esto podrá realizarse a través de la desconexión de los equipos informáticos o mediante un protector de pantalla protegido con contraseña que impida completamente la visualización de los datos personales. La reanudación del trabajo sólo será posible mediante la introducción de la contraseña.

El usuario no podrá cambiar la configuración de las aplicaciones y sistemas operativos de su puesto de trabajo sin la autorización de los responsables o administradores de seguridad informática y no podrá utilizar ninguna herramienta o utilidad no autorizada para acceder a los ficheros que contengan datos de carácter personal.

Está especialmente prohibido establecer cualquier tipo de conexión de datos a redes externas (como Internet) fuera de las establecidas y autorizadas por los responsables o administradores de seguridad informática.

Respecto al uso de ordenadores portátiles, PDA, smartphones y otros equipos, si el usuario precisa copiar en ellos archivos informáticos que contengan datos de carácter personal, solicitará la correspondiente autorización a los responsables o administradores de seguridad informática y velará, en la medida de lo posible, por su seguridad, controlando su ubicación y evitando su sustracción, además de utilizando siempre contraseñas de acceso al equipo u otros mecanismos equivalentes que eviten el acceso a los datos en caso de robo o pérdida accidental. Además, el usuario velará por eliminar dichos archivos a la que no sean precisos y por volcarlos a los sistemas informáticos principales en caso de que realice modificaciones en ellos al menos una vez a la semana.

En lo relacionado con los documentos en soporte papel, mientras éstos no estén archivados por estar en proceso de tramitación o revisión, el usuario deberá custodiarlos e impedir en todo momento que puedan ser accedidos por persona no autorizada (al finalizar la jornada laboral no deberán quedar a la vista documentos que contengan datos de carácter personal).

En el momento que hayan de ser eliminados deberá procederse a la destrucción de forma que se evite su recuperación posterior (mediante máquina destructora de papel o mecanismo equivalente).

En el caso de las impresoras, el usuario deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a dichos datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

3) Ficheros

El usuario recibirá instrucciones sobre los ficheros con datos de carácter personal que está autorizado a emplear, así como el tipo de acceso permitido (lectura, escritura, etc.) y la finalidad de los mismos. El usuario sólo podrá utilizar esos ficheros y únicamente de acuerdo con la finalidad estipulada, procurando además que los datos personales contenidos en ellos estén siempre actualizados y cancelándolos cuando ya no sean necesarios o pertinentes para la finalidad para la cual hubieran sido recabados, puesto que la normativa en materia de protección de datos prohíbe expresamente el mantenimiento indefinido de los datos de carácter personal.

En el supuesto de que el usuario desee crear ficheros propios o nuevos con datos de carácter personal, incluso de carácter temporal, deberá hacerlo previa autorización de los responsables o administradores de la seguridad informática, quienes le informarán de cualquier posible medida legal, técnica u organizativa que haya que adoptar. De igual forma deberán proceder si desea utilizar ficheros ya creados para una finalidad distinta de la existente hasta el momento o si desea añadir datos personales inicialmente no previstos en campos tipo "Observaciones" o similares.

4) Soportes y documentos

En caso de querer almacenar en cualquier tipo de soporte informático (disquete, CD o DVD, memoria USB, etc.) datos de carácter personal, sean nuevos o provenientes de otros ficheros, o de realizar cualquier operación de copia, aunque sea temporal, se deberá contar con la autorización de los responsables o administradores de la seguridad informática, quienes le informarán de cualquier posible medida de seguridad que haya que adoptar, incluyendo la obligación de etiquetar dichos soportes, catalogarlos y almacenarlos en lugares protegidos de acceso restringido. Lo mismo se aplicará en caso de querer sacar dichos soportes del local donde está su puesto de trabajo o de entrar soportes provenientes del exterior.

Los documentos impresos y soportes informáticos deben ser tratados y conservados con la máxima confidencialidad y, por tanto, deberán guardarse en sitios de acceso restringido al personal autorizado. También, cuando el usuario quiera reutilizar o desechar soportes informáticos que contengan datos de carácter personal aplicará un sistema que garantice la imposibilidad de acceder a los datos grabados con anterioridad, como un borrado total o un formateado.

5) Contraseñas

Cada usuario es responsable de la confidencialidad de su contraseña o de proteger cualquier otro mecanismo de autenticación equivalente y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá comunicarlo con la mayor brevedad posible a los responsables de los ficheros o a los administradores de la seguridad informática para proceder inmediatamente a su cambio así como para registrar la incidencia en el registro de incidencias. En el caso de que el código de usuario y la contraseña sean compartidos por varios usuarios, todos ellos son responsables por igual de mantener esa confidencialidad. En especial, queda prohibido escribir la contraseña en cualquier tipo de soporte físico (papel, etc.) o lógico (archivos).

El usuario está obligado a cambiar su contraseña cada 12 meses, y a asignar una nueva contraseña que siga las siguientes reglas: un mínimo de 6 caracteres; prohibición de repetir la misma contraseña de forma consecutiva o de utilizar secuencias lógicas de nuevas contraseñas; evitar los nombres comunes, números de matrículas de vehículos, teléfonos, fechas, nombres de familiares, amigos, etc., y derivados del nombre del usuario como permutaciones o cambio de orden de las letras, transposiciones, repeticiones de un único carácter, etc.

6) Copias de seguridad

En caso de que el usuario detecte que se han borrado por error, avería del sistema informático u otra razón datos, ficheros, bases de datos, etc. que contuvieran datos de carácter personal, deberá comunicarlo de inmediato a los responsables o administradores de la seguridad informática para que se proceda, en la medida de lo posible, a recuperar la copia de seguridad más reciente y para, inmediatamente después, proceder, en la medida de lo posible, a actualizar manualmente los datos que no estuvieran en dicha copia y se hubieran perdido.

7) Gestión de incidencias

La certeza o sospecha de que se ha producido una incidencia que entrañe riesgo para la seguridad de los datos personales debe ser comunicada a los responsables o administradores de la seguridad informática con la mayor celeridad posible. Entre otras, se consideran incidencias los olvidos o conocimiento por parte de usuarios no autorizados de las contraseñas, la creación de ficheros con datos de carácter personal no autorizados, la pérdida de los datos de un fichero o de los soportes que los contienen, la aparición de listados no controlados y, en general, cualquier incidencia que no permita acceder a los datos o permita acceder a los datos con un tipo de acceso teóricamente no permitido o a datos a los que no se debería tener acceso.

8) Datos especialmente protegidos

Se consideran datos especialmente protegidos los de religión, creencias, ideología sindical o política, vida sexual y salud. Estos datos precisan unas medidas de seguridad especiales y, en algunos casos, implican que hay que contar con la autorización expresa y por escrito de la persona de quien se recogen. El usuario se abstendrá de recoger cualquiera de estos datos sin consultar previamente con los responsables o administradores de la seguridad informática y deberá poner, por tanto, especial énfasis en controlar el tipo de datos que inserta en campos de observaciones y otros campos de texto libre de aplicaciones y bases de datos o en documentos y archivos en papel a los que tiene acceso.

En caso de transmitir estos datos especialmente protegidos por correo electrónico, Internet u otro tipo de servicio de telecomunicaciones, el usuario deberá contactar previamente con los responsables o administradores de la seguridad informática para determinar las especiales medidas de seguridad que cabe aplicar.

9) Cesiones y tratamiento por parte de terceros

Aparte de las cesiones de datos impuestas por la ley, los datos de carácter personal sólo pueden ser comunicados a un tercero previo consentimiento del interesado. Por ello, si, para la realización de cualquier tarea, el usuario quisiera comunicar a un tercero (sea empresa, profesional, administración pública, etc.) datos de carácter personal, deberá contactar previamente con los responsables o administradores de la seguridad informática para determinar su viabilidad y las especiales medidas de seguridad y jurídicas que hay que aplicar.

En el caso de subcontratar a terceras empresas la realización de trabajos que impliquen la necesidad de que éstas traten datos de carácter personal pertenecientes a los ficheros de BARBERÁN, será preciso regular este proceso mediante la formalización de un contrato en el que se estipulará el encargado del tratamiento, por lo que, también en estos casos, deberá contactarse previamente con los responsables o administradores de la seguridad informática.

10) Derechos de los afectados

Todas las personas de las que se disponga datos de carácter personal tienen, por ley, potestad para ejercer los derechos de acceso (conocer qué datos se tienen de él), rectificación (pedir su modificación), cancelación y oposición (pedir su baja total o parcial o restringir su utilización o posibles comunicaciones a terceros) de sus datos de carácter personal.

Es obligación de todo el personal contribuir al ejercicio de dichos derechos, por lo que los usuarios deberán redirigir cualquier consulta de este tipo a los responsables o administradores de la seguridad informática, quienes proporcionarán a ese individuo todas las explicaciones necesarias.

11) Acciones comerciales

La LOPD, la LSSI y la LGT imponen serias restricciones a la hora de realizar envíos publicitarios, tanto si se dirigen a personas físicas como si son genéricos. Por ello, en caso de querer realizar cualquier envío publicitario, sea por carta, correo electrónico, fax, SMS, etc., el usuario deberá consultar previamente la política establecida al respecto a su responsable.

12) Datos de candidatos

En caso de querer recibir información curricular de candidatos a empleos en BARBERÁN, el usuario deberá consultar previamente la política establecida al respecto a su responsable, puesto que dicha información es considerada especialmente sensible a efectos de la LOPD y debe protegerse adecuadamente. De igual forma, en caso de recibir currículo no solicitados, el usuario deberá borrarlos o, en todo caso, redirigirlos a su responsable o consultar con él sobre su posible conservación.

En ningún caso se procederá a reenviar dichos currículo a terceros (incluso entre empresas de un mismo grupo) sin la autorización previa del afectado. El usuario deberá consultar previamente con su responsable sobre la política establecida al respecto.

13) Cumplimiento

El incumplimiento de cualquiera de las obligaciones contenidas en el presente documento comportará las consecuencias jurídicas y laborales derivadas del propio incumplimiento cometido. Quien creara ficheros que contuvieran datos de carácter personal o desarrollara o instalara aplicaciones que permitieran tratarlos sin la correspondiente autorización será considerado responsable del fichero o de su tratamiento, con las consecuencias legales que de ello se derivan.