

8.1 LOPD: ELABORACIÓN DE UN DOCUMENTO INTERNO
8.1 DPBLO: BARNE-DOKUMENTUA LANTZEA



DATOS PERSONALES EN EL ENTORNO EMPRESARIAL, ¿QUÉ SON Y A QUÉ OBLIGA LA LEY?

DATU PERTSONALAK ENPRESAREN INGURUNEAN, ZER DIRA ETA ZERTARA BEHARTZEN DU LEGEAK?

Proteger los datos personales almacenados en soporte informático, es una obligación que no todas las empresas contemplan. La LOPD (Ley Orgánica de Protección de Datos de Carácter Personal) se extiende a todos los sectores y, por supuesto, es de necesario cumplimiento. Sin embargo, el desconocimiento y la falta de asesoramiento pueden señalarse como los factores que explican el bajo seguimiento de esta normativa.

Euskarri informatikoan jasotzen diren datu pertsonalak babestu behar dira, baina enpresa guztiek ez dute betebeharr hori aintzat hartzen. Datu Pertsonalen Babeserako Lege Organikoa (DPBLO) sektore guztietara zabaltzen da, eta, jakina, nahitaez bete behar da. Hala ere, ezjakintasunagatik eta aholkularitzaren gabeziagatik ez zaio asko jarraitu araudi horri.

Desde la aprobación de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), su grado de cumplimiento no presenta unos índices positivos; y gran parte de las empresas (que en su mayoría tratan información del tipo señalado) se exponen a ser sancionadas por tal motivo.

Datu Pertsonalen Babeserako 15/1999 Lege Organikoa onartu zenetik, lege horren betetze-maila ez da oso positiboa izan; eta enpresa gehienak lege hori ez betetzeagatik zigorrak jasotzeko arriskuan daude; izatez, enpresa gehienek adierazitakoaren moduko informazioa erabiltzen dute.

A continuación, se va a plantear un caso práctico que permita comprender mejor el ámbito de actuación y los requerimientos de la Ley:

Ondoren, jardun-esparrua eta Legearen eskakizunak hobeto ulertzeko aukera emango duen kasu praktikoa planteatuko da:

Hace cuatro años que Ana Odriozola es propietaria de una agencia inmobiliaria situada en el centro de Bilbao y en cuya oficina trabajan dos personas además de ella. Ciertamente, su empresa mantiene uno niveles significativos de operaciones; actuando como intermediaria en un importante volumen de ventas y alquileres efectuados en el ensanche bilbaíno.

Duela lau urtez geroztik, Bilboko hirigunean dagoen higiezinaren agentzia baten jabea da Ana Odriozola. Higiezinaren agentzia horren bulegoan beste bi pertsonak egiten dute lan. Bere enpresak eragiketa-maila handi samarra du, eta Bilboko zabalguneko higiezinaren salmenta eta alokairu askotan jardun du bitartekari gisa.

Desde el principio consideró las ventajas que los sistemas informáticos ofrecían a su actividad, y no dudó en equipar los puestos de trabajo de su oficina con ordenadores adecuados; encargando, al mismo tiempo, el desarrollo de una pequeña aplicación que permitiera gestionar su cartera de inmuebles y clientela de forma sencilla. Así, debido al destacado número de viviendas con el que ha trabajado y los años de funciona-

Hasiera-hasieratik hartu zuen aintzat sistema informatikoak oso onuragarriak zirela bere jarduerarako, eta bere bulegoko lanpostuak ordenagailu egokiekin hornitu zituen; era berean, bere higiezinaren zorroa eta bezeroak modu sinple batean kudeatzeko aukera emango zuen aplikazio txiki bat egin ziezaioten agindu zuen. Horrenbestez, enpresak lanean eman dituen urte horietan etxebizitza-kopuru handi batekin lan

miento de la agencia, la empresaria se encuentra en el momento actual con una "enorme" Base de Datos formada por cientos de registros (de la que se siente especialmente satisfecha, ya que en ella constata la evolución de su empresa). Como fundamentalmente se dedica a vivienda de segunda mano, cuenta con numerosos datos relativos a las personas propietarias y a la clientela con la que ha ejercido de intermediaria: nombre, apellidos, teléfonos, etc.

Otro ejemplo de su apuesta por la tecnología, es el sitio Web presencial con el que cuenta (en él presenta los servicios de la inmobiliaria); y a través del cual recoge comentarios y solicitudes de algunos clientes y clientas vía e-mail (mediante un formulario).

De igual modo, por las características de su trabajo, mantiene un contacto continuo con su abogada -y amiga- Josune García. Junto a ella, elabora los contratos y revisa diferentes aspectos legales relacionados con la actividad de la inmobiliaria; pero no tratan temas de gestión interna.

Uno de los días en los que ambas se encontraban reunidas, la empresaria comenta a la abogada la oferta que le había planteado otra inmobiliaria para trabajar en colaboración; compartiendo su cartera de viviendas y aunando esfuerzos en un área concreta de la ciudad. La abogada se interesa por las condiciones del futuro acuerdo y la información que van a intercambiarse, y ahí, es cuando por primera vez conoce el tipo de datos que la agencia almacenaba en su Base de Datos.

Inmediatamente, explica a su amiga que parte de los datos que almacena en ese fichero son de carácter personal: nombres, teléfonos, direcciones,... de personas propietarias y clientela; es decir, aportaban información sobre personas físicas concretas, y que, existe una Ley, que es de obligado cumplimiento para todas las empresas y profesionales que traten datos de este tipo: la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal). También le comunica que la infracción de tal normativa puede llegar a ser sancionada con cantidades elevadas que, en su caso, oscilarían entre un mínimo de 600 y un máximo de 60.000 euros. En ese momento, Ana recuerda que algo había oído hablar sobre ello, pero no había prestado mayor interés al entender que no almacenaba ninguna información con ese carácter...

Lógicamente, la empresaria no quiere perder más tiempo antes de adaptarse a los preceptos que fija la Ley; y así, contrata los servicios de la abogada para normalizar su situación al respecto, quien en primer lugar, comienza apuntando los procedimientos elementales que deben realizarse:

- Notificar y legalizar el fichero que contiene la Base de Datos ante la Agencia de Protección de Datos.
- Elaborar y aplicar en la inmobiliaria el Documento de Seguridad para cumplir con los requisitos legales e implantar una política de seguridad con arreglo al nivel de los datos contenidos en su aplicación.
- Redactar y aplicar las cláusulas y contratos que sean necesarios para obtener el consentimiento de la clientela y personas propietarias; y para notificar el tratamiento de datos por terceros (debido al acuerdo con la otra agencia se va a compartir dicha información). la Ley fija el deber de información; es decir, insta a proporcionar a las personas interesadas, bien en los diferentes documentos existentes, bien de forma verbal, cierta información cuando se

egin duenez gero, enpresaburuak ehunka erregistro biltzen dituen datu-base "itzela" du, eta oso harro dago, datu-base horrek enpresaren bilakaera islatzen baitu. Oro har, bigarren eskuko etxebizitzaren arloan dihardu, eta, hala, etxebizitza horien jabeen eta bezeroen buruzko datu ugari du; izena, abizenak, telefonoa...

Teknologiaren alde egin duen apustuaren beste adibide argi bat bere webgunean datza. Webgune horretan higiezin agentziako zerbitzuak aurkezten ditu, eta, bertan dagoen formulario baten laguntzaz, zenbait bezeroen iruzkinak eta eskaerak jasotzen ditu e-mail bidez.

Era berean, bere lanaren ezaugarriengatik, etengabe ari da harremanetan Josune García bere abokatu eta lagunarekin. Berarekin batera egiten ditu kontratuak eta berraztertzen ditu higiezin arloko jarduerarekin lotzen diren legezko alderdiak; alabaina, ez dute barne-kudeaketako gairik aztertzen.

Biak bilduta zeuden egun batean, beste higiezin agentzia batek elkarlanean jarduteko proposamena egin ziola aipatu zion enpresaburuak. Akordio horren arabera, bi higiezin agentziek beren etxebizitzaren zorroa partekatuko zuten, eta ahaleginak batuko zituzten hiriko oso ingurune zehatz batean. Abokatuak etorkizuneko akordio horren baldintzak eta trukaturako duten informazioa zein diren jakin nahi du, eta orduan jakin du, lehen aldiz, agentziak zein motatako datuak gordetzen dituen datu-basean.

Berehala argitzen dio bere lagunari fitxategi horretan gordetzen dituen datuen zati bat higiezin jabeen eta bezeroen datu pertsonalak direla: izenak, telefonoak, helbideak...; hau da, pertsona fisiko zehatzei buruzko informazioa dela, eta mota horietako datuak erabiltzen dituzten enpresak eta profesionalak nahitaez bete beharreko Lege bat dagoela, Datu Pertsonalen Babeserako Lege Organikoa. Halaber, aditza ematen dio araudi hori haustek kopuru handiko zigorrak eragin ditzakeela, eta bere kasuan, 600 euro eta 60.000 euro arteko zigorra izan daitekeela. Une horretan, Ana gogoratzen du halako zerbaite entzun zuela, baina, orduan, ez zuela arreta handirik jarri, bere ustez ez baitzuen halako informaziorik gordetzen ...

Logikoki, enpresaburuak lehenbailehen egokitu nahi du bere enpresa Legeak ezartzen dituen aginduetara; eta, horrenbestez, abokatuaren zerbitzuak kontratatzen ditu bere egoera normalizatzeko. Abokatuak, hasteko, jarraitu beharreko funtsezko prozeduraren berri ematen dio:

- Datuak Babesteko Agentziaren aurrean jakinaraztea datu-basean gordetzen duen fitxategia, horrek legeza dezan.
- Higiezin agentzian legezko baldintzak betetzeko segurtasun-dokumentua lantzea eta aplikatzea, eta bere aplikazioan dauden datuen mailaren arabeko segurtasun-politika aplikatzea.
- Bezeroen eta higiezin jabeen adostasuna lortzeko eta hirugarren batzuek datuak erabiltzen dituztenean jakinarazteko beharrezko klausulak eta kontratuak idaztea eta aplikatzea (beste agentzia horrekin egin beharreko akordioaren ondorioz informazioa partekatu egingo baita). Legeak informatzeko betebeharra finkatzen du, hau da, beren datuak jasotzen direnean, dokumentuen bitartez zein ahoz eman behar zaie guztiaren berri pertsona interesdunei. Hori dela eta, datuak jasotzean erabiltzen diren formularioak, legendak eta prozedurak berraztertu behar



recaban sus datos. Esta circunstancia obligará a revisar los formularios, leyendas y procedimientos que se emplean en la recogida de los datos; en concreto, deberá adaptar el formulario de contacto de su sitio Web.

Por ello, siguiendo la clasificación de datos que establece dicha ley, la inmobiliaria deberá adoptar las medidas de seguridad adecuadas a los datos personales de su clientela y personas propietarias que contienen su fichero informático (Base de Datos). En este caso, existen tres niveles:

- **Nivel básico:** Nombre, apellidos, direcciones de contacto (tanto físicas como electrónicas), teléfono (tanto fijo como móvil), otros datos de la misma índole...
- **Nivel medio:** Comisión de infracciones penales, comisión de infracciones administrativas, información de Hacienda Pública, información de servicios financieros...
- **Nivel alto:** Ideología, religión, creencias, origen racial, salud, vida privada...

En este sentido, la abogada le explica a Ana Odriozola, que hay que considerar el Real Decreto 994/1999; es decir la norma estatal que comprende el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal. Ésta, tiene por objeto establecer las medidas de seguridad de tipo técnico y organizativo relativas a los ficheros de datos; pero no sólo a ellos, sino también a los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en su tratamiento automatizado.

De este modo, en dicho Decreto, se señalan las medidas de seguridad obligatorias en el **nivel básico** (requerimientos mínimos que deberá cumplir la inmobiliaria atendiendo a los datos personales que almacena). A continuación, se detallan algunas de éstas:

- Documento de seguridad. La Ley recuerda que la persona responsable de seguridad será la encargada de elaborar e implantar la normativa de seguridad mediante un documento, que será de obligado cumplimiento para el personal con acceso a los datos de carácter personal.
- Documentar las funciones que desempeñará y obligaciones que asumirá cada persona trabajadora con acceso a los datos.
- Mantener una relación actualizada de personas usuarias con acceso autorizado; y controlar al mismo tiempo cuándo y a qué información acceden.
- ...

La abogada comunica a la empresaria que el *documento de seguridad* es una de las partes fundamentales de la protección de datos. Se trata del documento mediante el cual se elabora y adoptan las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal; siendo su adopción de obligado cumplimiento para la persona responsable del fichero (la empresaria), o en su caso, de la persona encargada del tratamiento.

De este modo, se deberá redactar obligatoriamente dicho documento, el cual tendrá que recoger como mínimo (dado el nivel de los datos) la siguiente información:

- Ámbito de aplicación del documento.
- Determinación de los ficheros de carácter personal (estructura, uso, cesiones previstas, forma de obtención de datos...).

dira; zehazki, bere webguneko harremanetarako formularioa egokitu beharko da.

Hortaz, Lege horretan ezartzen den datuen sailkapenari jarraituz, higiezin agentziak bere fitxategi informatikoan (datu-basean) jasotzen diren bere bezeroen eta higiezin jabeen datu pertsonaletarako segurtasun-neurriak finkatu beharko ditu. Kasu horretan, hiru maila daude:

- **Oinarrizko maila:** izena, abizenak, harremanetarako helbideak (fisikoak zein elektronikoak), telefonoa (telefonía finkokoa zein eskukoa), antzeko beste datu batzuk...
- **Maila ertaina:** arau-hauste penalak egin izana, arau-hauste administratiboak egin izana, Ogasun Publikoaren informazioa, finantza-zerbitzuen informazioa...
- **Maila handia:** ideologia, erlijioa, sinesmenak, arrazajatorria, osasuna, bizitza pribatua...

Ildo horretan, abokatuak argitzen dio Ana Odriozolari 994/1999 Errege Dekretua hartu beharko dela aintzat, hau da, datu pertsonalak dituzten fitxategi informatikoetarako Segurtasun Neurri buruzko Erregelamendua hartu beharko dela kontuan. Erregelamendu horretan datu-fitxategien segurtasun-neurri teknikoak edo antolamendukoak ezartzen dira, baita datu horien tratamenduan esku hartzen duten tratamendu-zentroenak, lokalenak, ekipoenak, programenak eta pertsonenak ere.

Hala, Dekretu horretan, **oinarrizko mailan** ezinbestean bete behar diren segurtasun-neurriak adierazten dira, higiezin agentziak biltzen dituen datuen arabera bete beharko diren gutxieneko baldintzak, hain zuzen ere. Ondoren, horietako batzuk zehazten dira:

- Segurtasun-dokumentua. Legeak gogorarazten du segurtasunaz arduratzen den pertsonak dokumentu baten bitartez landu eta ezarri beharko duela segurtasun-araudia. Segurtasun-dokumentu hori nahitaez bete beharko dute datu pertsonalak eskura ditzaketengatik langileek.
- Datuak erabil ditzakeen langile bakoitzak bete beharreko funtzioak eta bere gain hartuko dituen betebeharrak dokumentatzea.
- Datu horiek erabil ditzaketengatik pertsonen zerrenda eguneratua mantentzea, eta, aldi berean, zer informazio eskuratu duten eta noiz egiten duten kontrolatzea.
- ...

Abokatuak enpresaburuari jakinarazten dio *segurtasun-dokumentua* datuen babeserako funtsezko alderdietako bat dela. Dokumentu horretan lantzen eta finkatzen dira datu pertsonalen segurtasuna bermatzeko beharrezko neurri teknikoak eta antolamendu-neurriak, eta neurri horiek nahitaez bete beharko ditu fitxategiaz arduratzen den pertsonak (enpresaburuak), edo, hala badagokio, datu horien tratamenduaz arduratzen den pertsonak.

Horrenbestez, ezinbestean idatzi beharko da dokumentu hori, eta, datuen maila kontuan izanik, gutxienez honako informazioa jaso beharko da bertan:

- Dokumentuaren aplikazio-esparrua.
- Fitxategi pertsonalak zehaztea (egitura, erabilera, aurreikusten diren lagapenak, datuak lortzeko modua...).
- Segurtasun-planaren esparrua finkatzea, hau da, datu pertsonalak dituzten fitxategiak zehaztea, baita horiek

- Determinación del ámbito del plan de seguridad; es decir, detallar los ficheros que contienen datos personales, los ordenadores o equipos que los almacenan, el lugar en el que se ubican estos últimos, las personas que intervienen en el tratamiento de los datos, ...
- Establecimiento de un conjunto de medidas que garanticen la seguridad de los archivos informáticos y el tratamiento de datos de carácter personal.
- Detalle de las obligaciones y funciones derivadas del documento de seguridad, tanto para la persona responsable del fichero, como para las personas usuarias que manejan las aplicaciones.
- Los contratos con otras empresas que impliquen la prestación de servicios en los que estén involucrados datos de carácter personal.

Asimismo, el documento deberá estar actualizado en todo momento, a la vez que deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Por otro lado, exige la normativa que el documento se adecue, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. En este punto, la abogada insiste en que se considera una infracción grave "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen" (LOPD).

gordetzen dituzten ordenagailuak edo ekipoak, azken horiek kokatzen diren lekua, datuen tratamenduan esku hartzen duten pertsonak, eta abar ere.

- Artxibo informatikoen segurtasuna eta datu pertsonalen tratamendua bermatuko duten neurriak ezartzea.
- Segurtasun-dokumentuaren ondoriozko betebeharrak eta funtzioak zehaztea, bai fitxategiaz arduratzen den pertsonarentzat, bai aplikazioak erabiltzen dituzten pertsona erabiltzaileentzat.
- Beste enpresa batzuekin egiten diren kontratuak, baldin eta datu pertsonalen erabilera eskatzen duten zerbitzuak egin behar badira.

Era berean, dokumentuak beti egon beharko du eguneratuta, eta informazio-sisteman edo informazioaren antolamenduan aldaketa handiak egiten diren guztietan berraztertu beharko da dokumentua. Bestalde, araudiak eskatzen duenez, dokumentua beti egokitu beharko zaie datu pertsonalen segurtasunaren arloan indarrean dauden xedapenei. Ildo horretan, abokatuak nabarmendu egiten du Datu Pertsonalen Babeserako Lege Organikoak arau-hauste larritzat jotzen duela datu pertsonalak dituzten fitxategiak, lokalak, programak edo ekipoak arauz ezartzen diren segurtasun-baldintza egokirik gabe mantentzea.

En primer lugar, las empresas deben ser conscientes del carácter de los datos que almacenan y de los requerimientos planteados por las leyes en cada caso. La despreocupación o falta de interés en este sentido, conllevará desenlaces no deseados ("problemas" con la justicia).

Ciertamente, cumplir con las obligaciones que fija la LOPD -en la mayoría de las ocasiones- no es una tarea laboriosa; y, sin duda, será más apropiado adecuarse a los dictados de la Ley que recibir una sanción por lo contrario. Con seguridad, el coste de lo primero será significativamente inferior al importe a pagar por incumplimiento de la normativa. Además, la imagen de aquella empresa que cumple la Ley queda reforzada.

Lehenik, enpresek biltzen dituzten datuen izaeraren eta legeek kasu bakoitzean planteatzen dituzten eskakizunen jakinaren gainean egon beharko dute. Arlo horretako arduragabetasunak edo interes gabeziak nahi ez diren ondorioak izango ditu (justizia-rekin "arazoak").

Izan ere, Datu Pertsonalen Babeserako Lege Organikoak finkatzen dituen betebeharrak betetzea, gehienetan, ez da zaila izaten; eta, inolako zalantzarik gabe, egokiago izango da Legeak agintzen duenera moldatzea, ez egokitzeagatik zigorra jasotzea baino. Zaude ziur lehenengoaren kostua askoz ere txikiagoa izango dela araudia ez betetzeagatik ordaindu beharreko zenbatekoa baino. Gainera, Legea betetzen duen enpresaren irudia indartu egingo da.