- **Procedimiento Nº: E/06746/2020**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes:

HECHOS

PRIMERO: Las actuaciones de inspección se inician por la recepción de una reclamación sobre una brecha de seguridad de los datos personales con las siguientes características:
Fecha de entrada de la reclamación: 27 de febrero de 2020.
Reclamante: ***A.A.A.*** (en adelante, el reclamante)
Reclamada: LEROY MERLIN ESPAÑA, S.L., con NIF B84818442 y domicilio en Avda. de la Vega, 2 - 28108 Alcobendas (Madrid).
Hechos según manifestaciones del reclamante:
- Al disponerse a crear una cuenta de usuario para dos compañeros de trabajo suyos (con su autorización) en el portal web de LEROY MERLIN ESPAÑA S.L., de URL ******URL.1***, el reclamante descubre con sorpresa que el portal ya disponía de sus datos personales (nombre, apellidos, dirección postal y número de teléfono), los cuales no han sido introducidos en el proceso de registro.
- El alta en la aplicación web requiere introducir una dirección de correo electrónico y un DNI. Únicamente conociendo este último, es suficiente para acceder al área privada de su titular y consultar sus datos personales asociados.
- El reclamante sospecha que los datos personales proceden del sistema de fidelización de clientes que tiene la empresa mediante tarjeta, la cual es gratuita de realizar y para cuya tramitación hay que cumplimentar un boletín con datos de carácter personal.
- El reclamante solicita que se investiguen los extremos indicados, al estar vigente el problema a fecha 21/02/2020, y se desconoce el número de afectados y el tiempo que lleva ocurriendo esta situación.

Documentación aportada:

-DVD con 2 vídeos de pruebas realizados el 21/02/2020 por el reclamante a las 19:00 aproximadamente, donde se comprueba como al realizar el registro con DNI y correo electrónico, tras confirmar el mismo, aparecen datos de carácter personal, sin haber introducido ninguno de ellos durante el proceso.

Los antecedentes que constan en los sistemas de información son los siguientes:

Con fecha 03/07/2020 en los registros de entrada 023303/2020 y 023306/2020, asociado a la Admisión de Trámite E/03360/2020, la Agencia Española de Protección de Datos (en adelante, AEPD) obtuvo respuesta del Delegado de Protección de Datos de LEROY MERLIN después del oportuno traslado de la reclamación. Tras ello, se

propuso para la investigación como una brecha de seguridad y fue aceptada por los siguientes motivos:
- Potencial ocurrencia de brecha de seguridad del tipo acceso no autorizado a datos personales de usuarios de la web de LEROY MERLIN.
- Existencia de evidencias para el requerimiento de cierto análisis de seguridad del tratamiento y del principio de confidencialidad en el procedimiento de alta de usuarios en la web de LEROY MERLIN
- Necesidad de aclaración sobre el proceso de cesión de datos personales de AKÍ BRICOLAJE ESPAÑA, S.L.U. (en adelante, AKÍ), antigua marca, a LEROY MERLIN en su absorción empresarial.
- Potencial uso indebido por definición interna de datos personales adquiridos por LEROY MERLIN para otras finalidades.

ENTIDAD INVESTIGADA:

LEROY MERLIN ESPAÑA, S.L. (en adelante, la investigada), con NIF B84818442 y domicilio en AVDA. DE LA VEGA, 2 - 28108 ALCOBENDAS (MADRID).

SEGUNDO: En fecha 21 de agosto de 2020, se solicita información a la investigada sobre los hechos manifestados por el reclamante en relación con la brecha de seguridad puesta en conocimiento a la AEPD:

Haberse detectado presuntas carencias en la seguridad de los datos personales de sus clientes para la realización del alta como usuarios en su dominio ******URL.1****, en el que, entre otros, se producen actividades de comercio electrónico (compraventa de sus productos).*

De la respuesta de la investigada recibida el 05/09/2020 se desprende lo siguiente:

Respecto del mecanismo y procedimiento por el que se registran usuarios en la web de la entidad:

- Todo según manifestaciones de la investigada:
    - Resulta necesario incorporar los datos personales DNI / NIE / Pasaporte y correo electrónico para proceder al registro y validación en el portal web ******URL.1***.
    - Habiéndose aceptado el “Aviso Legal” y la “Política de Privacidad” se ha de verificar la cuenta mediante acceso al correo electrónico proporcionado, en un proceso de dos pasos.
    - Una vez validada la cuenta web, queda finalizado el proceso de registro y el usuario puede acceder a su espacio en el portal web.
    - Toda la información personal de los clientes se registra y vincula a una ficha única para cada cliente y usuario. Siendo “REFCLI” la base de datos de la investigada en que se contiene datos de sus clientes.
    - Las aplicaciones y herramientas de la investigada, físicas y digitales, modifican, con los permisos oportunos, la base de datos “REFCLI”.
    - Se requiere información veraz, cierta y sobre la persona concreta que realiza el alta según se identifica en el Régimen de Garantías y

Responsabilidades en el correspondiente “Aviso Legal” de la investigada.

Medidas técnicas y organizativas de seguridad implementadas con anterioridad a la detección de la brecha de seguridad:

- La investigada informa que su base de datos de clientes se encuentra alojada en el CPD de Telefónica (Alcalá Datacenter) bajo las medidas de seguridad correspondientes a un Tier IV.
- La investigada expone que dispone de una “Política de control de accesos” por la que se establece el protocolo de acceso a los directorios.
- La investigada manifiesta que el conjunto de sistemas de información que dan soporte a los procesos de usuario, procesos de soporte IT y procesos de gestión de IT operan bajo el “Marco Normativo de Seguridad de la Información” así como que dicho sistema de gestión de información, que incluye los procesos vinculados, está certificado bajo el estándar de seguridad ISO 27001 (se aporta evidencia).

Medidas técnicas y organizativas realizadas con objeto de minimizar los efectos adversos de la brecha de seguridad y hasta su resolución final:

- La investigada aporta evidencia de los correos electrónicos emitidos por su parte el 2 de julio de 2020 a los titulares de las cuentas de dirección electrónica usadas por el reclamante: ******EMAIL.1*** y ******EMAIL.2***, en los que, en el ámbito de la Admisión de Trámite E/03360/2020 de la AEPD, les informó de los datos personales que obraban en sus sistemas y la forma en que éstos habían sido incorporados a su sistema previamente al registro pretendido por el reclamante.
- La investigada expone que el campo DNI / NIE / Pasaporte se considera “clave” con la pretensión de recuperar todas las transacciones de sus clientes y usuarios en la web y poder mostrarles, en consecuencia, en su área privada del portal, los puntos generados con sus compras y los cheques de fidelidad disponibles; mejorando, a su vez, la experiencia cliente en su proceso de alta.
- La investigada informa que sus fichas de datos personales de clientes, almacenadas en REFCLI, pueden no tener asociada una cuenta de correo electrónico. Añade la investigada que su herramienta de facturación, incluso, permite la gestión y expedición de facturas sólo con: nombre, primer apellido, dirección postal y DIN / NIF (no es necesario ni segundo apellido, ni teléfono de contacto ni correo electrónico).

Medidas técnicas y organizativas ejecutadas para evitar la ocurrencia de la brecha de seguridad en el futuro:

- La investigada informa haber procedido a ciertos cambios en su portal web para evitar una brecha de seguridad como la acontecida, esto ha supuesto en términos generales un:

    - Nuevo flujo de datos personales para el registro en el portal web, basado en la relación entre el DNI y su existencia en la base de datos

REFCLI, para posteriormente valorar si existe dirección de correo electrónico del cliente.

- La investigada detalla que el nuevo flujo de datos contempla:
  - Una nueva lógica del proceso de registro en el portal web que comprueba previamente la existencia de DNI / NIE / Pasaporte en su base de datos REFCLI:
    - En caso negativo, se continua normalmente con el registro del resto de datos personales en REFCLI.
    - En caso positivo, se valida si existe una cuenta de correo electrónico asociada al cliente o usuario:
      - En caso de que exista la cuenta de correo electrónico y ésta coincida con la introducida con la cuenta o cuentas asociadas en REFCLI, entonces se permitirá completar el registro en el portal web al cliente / usuario.
      - En caso de que no exista cuenta de correo electrónico, se le muestra un mensaje al cliente / usuario para que contacte con el departamento de atención al cliente de la investigada en ******EMAIL.3*** para la validación de sus datos personales y posterior registro, si procede (comprobación por solicitud de copia de DNI / NIE / Pasaporte de si los datos se corresponden con el titular de la información que ya se dispone en REFCLI).
      - En caso de que existe cuenta de correo electrónico y no coincida con dicha existente, se seguirá el mismo procedimiento que si no existiera la misma, es decir, se requerirá comprobación del titular de los datos personales. Si hubiera varias cuentas de correo electrónico, se procederá con cada una de ellas según la forma expuesta en estos tres apartados.

<u>Respecto al proceso de cesión de datos personales de clientes de AKÍ a la entidad en la absorción empresarial acometida:</u>

- La investigada señala como antecedentes al proceso de cesión de datos personales de AKÍ a su entidad que el 1 de enero de 2019 se produjo, por sucesión universal, la adquisición de la totalidad de los bienes, derechos y obligaciones del patrimonio de AKÍ y que se subrogó en su posición ante terceros.
- La investigada detalla que los datos personales incluidos en el programa de fidelidad “SinFin" de AKÍ se realizó al amparo de las condiciones legales firmadas en el contrato de cesión de la base de datos “SinFin”, firmado en Madrid entre las partes, el 5 de febrero de 2018 (se aporta copia de dicho contrato) y al amparo de los plenamente vigentes en ese momento *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* y *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*.

- La investigada expone que la empresa AKÍ contaba en su base de datos con aproximadamente 1,5 millones de clientes identificados y pertenecientes al programa “SinFin”.
- La investigada aporta copia de las condiciones del programa “SinFin" de AKÍ referidas a los datos personales de sus clientes o usuarios, en que se explicita literalmente:

  "Mediante la aceptación de estas condiciones, el socio consiente expresamente la cesión o comunicación de los datos incluidos en el fichero o ficheros anteriormente referidos, a las empresas del grupo ADEO, ya constituidas o por constituir, con independencia de la enseña o marca bajo las que operen las mismas, con las mismas finalidades que se han indicado para la recogida de datos por AKÍ Bricolaje España. Dichas empresas se dedican a la venta al por menor de artículos de bricolaje, jardinería, decoración y construcción, que en algún caso puede desarrollarse bajo el régimen denominado “descuento duro” o “hard discount”.
- La investigada añade que en el proceso de fusión empresarial 300.000 clientes del programa “SinFin” de AKÍ no consintieron la cesión de sus datos por haberse opuesto según una de las cláusulas de las condiciones del programa (se aporta copia de éstas, como se ha reseñado anteriormente).
- La investigada incorpora documentación sobre su plan de comunicación a clientes sobre la fusión del programa “SinFin” de AKÍ al “Club Leroy Merlin”, estableciendo que dicha campaña de comunicación contemplaba:

  - Acción comercial, en ventajas y beneficios para clientes.
  - Existencia de un fichero para el tratamiento de datos personales y finalidad de éstos.
  - Otorgar la posibilidad de ejercer derechos vigentes en el momento de protección de datos.
  - Adjuntar bases legales.
  - Opción de darse de baja de recibir correos electrónicos.
  - Identificación de la cesión de datos personales de AKÍ e identificación de la investigada como responsable del tratamiento.

- La investigada informa de que la acción de comunicación de la base de datos al programa se realizó con la siguiente metodología:
  - Análisis de la situación inicial de ambos programas de fidelidad con el detalle de diferencias y similitudes.
  - Establecimiento de los planes de acción correspondientes según las siguientes líneas de actuación (aspectos de negocio, aspectos legales, aspectos técnicos y plan de comunicación).
  - Análisis de resultados de la integración.

- La investigada manifiesta haber analizado el impacto de la integración de bases de datos para garantizar:
  - El mantenimiento de las bases de datos de clientes tras la integración de ambas compañías.
  - Una gestión centralizada de los clientes durante todo el proceso por parte de la investigada sobre protección de datos personales.

- El acompañamiento sincronizado con la integración de las tiendas.
- La definición de un plan de comunicación conjunto evitando sobre impactos.
- La creación de un plan de contingencia para atender las posibles preguntas y dudas de los clientes en todo lo relativo al proceso.
- La operativa de todas las tiendas para poder seguir atendiendo el negocio (devoluciones y gestión de las garantías de los productos comprados en las tiendas integradas).
- La aplicación de los beneficios obtenidos en el programa una vez integradas las tiendas.

- La investigada señala que el plan de comunicación se prolongó aproximadamente tres meses, comenzando en marzo de 2018, para cumplir con el deber de información y otorgando la posibilidad de darse de baja al socio. En dicha comunicación, la investigada expresa que pretendió:

    - Comunicar a los clientes acerca de la unión de ambas marcas, informándoles de su integración y adjuntando, a estos efectos, su numeración de socio.
    - Adjuntar las condiciones del programa de fidelidad correspondiente, dando la posibilidad de solicitar la baja en el mismo.
    - Informar al cliente de las cláusulas legales alegadas para realizar su inclusión en la nueva Base de Datos.
- La investigada expresa que el plan de comunicación de la cesión de datos personales se ejecutó en dos fases, repartidos por tiendas. En primera instancia, se comunicó a los clientes de las tiendas de Colmenar Viejo, Talavera de la Reina y Figueres, y posteriormente al resto de clientes de tiendas AKÍ (se aportan evidencias de ambas fases).
- La investigada presenta documentación sobre la información de adecuación al nuevo marco normativo europeo sobre protección de datos [*Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*, en adelante, RGPD] remitida a todos los clientes el 2 de mayo de 2018.
- La investigada aporta una copia del *planning* completo de comunicación llevado a cabo en el proceso de absorción.

<u>Legitimidad y periodo de conservación de los datos personales de sus clientes para autocompletar el alta de usuario a partir de los otorgados para la generación de facturas de compra:</u>

- La investigada manifiesta que los datos personales requeridos a sus clientes para cuestiones de facturación referidas a compras realizadas en su entidad, tanto físicas como digitales, son tratados única y exclusivamente para la finalidad de poder dar cumplimiento a la correcta gestión y expedición de las correspondientes facturas solicitadas por los interesados.
- La investigada aclara sobre la configuración técnica de sus entornos, sus aplicaciones y sus herramientas que cuando un cliente solicita la emisión de

una factura tras una compra en su entidad, si no constan sus datos personales, éstos son recabados únicamente para la generación y expedición de facturas y se le consulta si quiere que sean registrados, conservados y almacenados para la gestión ágil de solicitudes similares en el futuro y para la incorporación en REFCLI.

- La investigada alega que la base de legitimación para la gestión y expedición de las facturas de compras es el cumplimiento de una obligación legal según el artículo 5.1.c) del RGPD y para la custodia de sus datos para futuras facturas es el consentimiento libre y voluntario otorgado por el interesado. La investigada aporta copia del reverso de las facturas expedidas en la actualidad en que se menciona lo referente a protección de datos personales en su apartado 38.
- La investigada incorpora tres capturas de pantalla en que representa el proceso de generación y creación de cuentas para la facturación a sus clientes, el cual comienza por una búsqueda en la base de datos, incorporación por consentimiento del cliente en la base de datos y creación de la ficha de cliente en REFCLI.
- La investigada expresa que en la gestión y expedición de las facturas a partir de los datos personales aportados por sus clientes observa los principios de minimización de daros y de limitación de la finalidad, y que ante estos clientes se presenta como responsable del tratamiento. La investigada insiste en que el correo electrónico y el teléfono (fijo o móvil) queda a discreción del interesado para esta cuestión.
- La investigada sostiene disponer de interés legítimo y la existencia de expectativa de los clientes en cuanto al uso y tratamiento posterior de sus datos personales para autorrellenar los campos del área privada en el momento de darse de alta en el portal web. La investigada añade que esta recuperación sólo puede tener lugar si los clientes han consentido la captación y custodia de sus datos en REFCLI.
- La investigada alega que lo anterior tiene cabida legal en el artículo 6.1.f) del RGPD y manifiesta haber efectuado una evaluación meticulosa de ponderación entre el interés legítimo de mi representada y los intereses o derechos fundamentales de los clientes.
- La investigada expresa que de la evaluación de interés legítimo realizada se ha concluido que prevalecen sus intereses legítimos para el tratamiento frente al posible impacto para los derechos y libertades fundamentales de los interesados debido a que:
    - La investigada dispone de interés en poder mejorar la experiencia de los clientes durante su proceso de registro y alta en el portal web, recuperando todas sus transacciones y mostrando sus puntos generados en las compras y los cheques de fidelidad disponibles en el proceso de alta.
    - La investigada valoró la propia necesidad del tratamiento para poder prestar ese servicio de mejora de experiencia del cliente.
    - La investigada valoró garantías adicionales para impedir cualquier impacto indebido sobre los interesados.

La investigada establece que el mantenimiento de una única base de datos, REFCLI, responde a:

- Razones de índole técnica y de seguridad.
- Razones de satisfacción y mejora en la experiencia usuaria de sus entornos y ecosistemas digitales y usabilidad de éstos por parte los clientes.

La investigada concluye que el interés legítimo es válido con esta ponderación de intereses y señala el considerando (47) del RGPD a título ejemplar de este caso.
La investigada establece que, a pesar de la conclusión obtenida y para profundizar, se otorgó las recomendaciones de:

- Incluir la finalidad en el registro de actividades del tratamiento (RAT).
- Modificar la información básica relativa al tratamiento de los datos de los usuarios incluyendo la finalidad y ofreciendo una explicación sobre el origen de los datos de los usuarios.
- Configurar el área privada de los usuarios cuyo DNI consté en REFCLI para que en el primer acceso tras el registro se pregunte al usuario si desea validar los datos sugeridos o, en su defecto, validar en el formulario de registro las categorías de datos que se pudieran recuperar.

- La investigada expresa que el criterio de conservación de los datos generados en la facturación se encuentra en la segunda capa de política de privacidad ubicada en ******URL.2*** y que esto se expresa en la información básica sobre protección de datos de las facturas (se aporta copia de reservo de las facturas, como se ha reseñado anteriormente).

- La investigada informa que los clientes que acceden a que sus datos personales sean almacenados para futuras necesidades de facturación se atienen a lo dispuesto en la política de privacidad al efecto, literalmente:

  "Los datos personales proporcionados por los Usuarios se conservarán mientras no se solicite su supresión por el interesado. En caso de inactividad, LEROY MERLIN conservará los datos de carácter personal facilitados por los Usuarios por un período máximo de cinco (5) años, sin perjuicio de la posibilidad de ejercer sus derechos en los términos que se indican más adelante.
  En todo caso, el plazo de conservación de los datos vendrá marcado por la normativa mercantil, contable y fiscal u otra normativa vigente que establezca de manera obligatoria un plazo de conservación mayor a los anteriores"

  La investigada concluye que conserva los datos de los clientes y usuarios mientras éstos no requieran lo contrario o procedan a su edición en el portal web, mientras que, respecto a las facturas emitidas, cumpliendo con la normativa fiscal, se almacenan durante cinco años ante eventuales necesidades de duplicados necesarios y solicitados por los interesados.

<u>Finalidades para las que se recogen los datos personales de sus clientes:</u>

- La investigada manifiesta que la recuperación y volcado de la información personal de los clientes registrada en REFCLI se ampara en el interés legítimo, actuando ella como responsable del tratamiento y sus clientes como interesados.

- La investigada informa de que, para reforzar el cumplimiento de los principios relativos a la protección de datos en el tratamiento de datos de sus clientes, se trabaja en la implementación de las siguientes medidas:

    - Actualización de una nueva política de privacidad (segunda capa de la información sobre protección de datos): incluir mención expresa al tratamiento de datos personales a partir de información personal de clientes y usuarios en establecimientos físicos o digitales de la investigada.
    - Actualización del email de bienvenida: el correo electrónico es remitido tras validarse la cuenta web del usuario, por alta y registro en el portal de la investigada.

    - Actualización de la información básica sobre la protección de datos para las facturas emitidas por la investigada.

    - Actualización del RAT, en concreto en su apartado “web” para contemplar las novedades en el funcionamiento de alta y registro en REFCLI.

- La investigada expone estar trabajando para que si en el proceso de facturación un cliente aporta datos personales más allá de los estrictamente necesarios (como número de teléfono y/o dirección de email), éstos quedarán identificados en REFCLI. Si posteriormente, el usuario o cliente optase por registrarse en el portal web de la investigada, se le mostrará como ventana emergente recuperar los datos personales existentes en REFCLI, configurar los consentimientos para el envío de comunicaciones comerciales y modificar sus datos personales. En caso de no atender a dicha ventana emergente, los datos personales del cliente recabados serán tratados a los efectos del registro en el portal.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las “*violaciones de seguridad de los datos personales”* (en adelante quiebra de seguridad) como *“todas aquellas violaciones de la*

seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

En el presente caso, se produjo una brecha de seguridad de los datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad como consecuencia del acceso no autorizado a datos personales de usuarios de la web de LEROY MERLIN.

El artículo 32 del RGPD señala lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.".

El citado artículo contempla que "*el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".* No adopta una relación cerrada de medidas técnicas y organizativas, sino que éstas deberán ser las apropiadas en función del nivel de riesgo previamente analizado.

En consecuencia, se trata de determinar si las medidas técnicas y organizativas eran las adecuadas al nivel de riesgo predeterminado, así como la diligencia en la reacción ante una brecha de seguridad y, en su caso, las medidas adoptadas para evitar que en el futuro pueda repetirse una incidencia de similares características que pueda comprometer los derechos y libertades de los interesados.

De las actuaciones de investigación se desprende que LEROY MERLIN disponía de medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencia pero, sin embargo, se produjo la incidencia ahora analizada.

Asimismo, disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido, tras una reclamación de un ciudadano, la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

También debe valorarse la adopción de medidas técnicas y de gestión, como son los cambios efectuados en su portal web mediante un nuevo flujo de datos personales que contempla una nueva lógica del proceso de registro al objeto de comprobar y en su caso mejorar la gestión de datos personales.

En consecuencia, se debe concluir que la entidad investigada disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente mediante la implementación de medidas tales como la actualización de una nueva política de privacidad, del email de bienvenida, de la información básica sobre la protección de datos en relación a las facturas emitidas y la actualización del Registro de Actividades de Tratamiento en su apartado “web”. Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada causada previsiblemente por un error puntual.

III

A la vista de las actuaciones practicadas, se ha acreditado que la actuación de la entidad investigada como entidad responsable del tratamiento de los datos personales ha sido proporcional y acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a LEROY MERLIN, S.L. con NIF B84818442, y con domicilio en Avda. de la Vega, 2, 28108 Alcobendas, Madrid.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-0419

Mar España Martí
Directora de la Agencia Española de Protección de Datos