- **Expediente N.º: EXP202406971**

- RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR RECONOCIMIENTO DE RESPONSABILIDAD Y PAGO VOLUNTARIO

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 7 de noviembre de 2025, la Presidencia de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***MAJOREL SP SOLUTIONS, S.A.*** (en adelante, ***MAJOREL SP SOLUTIONS, S.A.***), mediante el acuerdo que se transcribe:

<<
Expediente N.º: EXP202406971

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes,

HECHOS

PRIMERO: La Agencia Española de Protección de Datos ha tenido conocimiento de ciertos hechos que podrían constituir una posible infracción imputable a ***MAJOREL SP SOLUTIONS, S.A.*** con NIF **A82112665** (en adelante, MAJOREL SP SOLUTIONS, S.A.).

Los hechos que se pusieron en conocimiento de esta autoridad fueron los siguientes:

El 15/01/2024, MAJOREL SP SOLUTIONS, S.A. comunicó a la representación legal de los trabajadores, que iba a comenzar a prestar servicio a la compañía ******EMPRESA.2***.

Se afirma que el 6/02/2024, cuando ya había trabajadores que prestaban servicio a ******EMPRESA.2***, MAJOREL SP SOLUTIONS, S.A., les envió un documento con las características generales del contrato mercantil suscrito por ambas partes, del que la denunciante destaca el párrafo: "*Los datos personales de los representantes, empleados o cualquier otra persona que actúe en nombre y representación de cada parte, y que sean proporcionados a la otra parte para el desarrollo y ejecución del contrato, serán tratados por la parte destinataria exclusivamente para la ejecución, gestión y control del contrato, y el cumplimiento con las correspondientes obligaciones legales y en concreto el RGPD*".

La denunciante expresa que tal documento solo está firmado por la representante de Recursos Humanos de MAJOREL SP SOLUTIONS, S.A., además de no incluir

información sobre el consentimiento para transferir datos a una empresa internacional (***EMPRESA.2**).

Sostiene que, durante la formación a los trabadores, MAJOREL SP SOLUTIONS, S.A. solicitó a estos sus números de teléfono para asegurarse que los tenían actualizados. La solicitud se realizó en un folio en blanco, en el que los trabajadores presentes en la formación anotaron su número de teléfono personal y fecha de nacimiento, indicándole con posterioridad MAJOREL SP SOLUTIONS, S.A. que sería en ese número de teléfono en el que recibirían las contraseñas para usar los aplicativos del cliente. No se les entregó documento alguno que acreditaba los derechos de cesión de esos datos, ni el fin ni la solicitud de autorización expresa al trabajador para ceder los datos.

La denunciante indica también que algunos trabajadores han recibido en sus teléfonos móviles, mensajes de ***EMPRESA.2** con los datos de acceso a los aplicativos informáticos, deduciendo que ha sido MAJOREL SP SOLUTIONS, S.A. la que ha cedido los números de teléfono de los trabajadores a aquella, sin previa consulta ni autorización.

Señala la denunciante además que las dos secciones sindicales enviaron correos electrónicos a la representante de RRHH de MAJOREL SP SOLUTIONS, S.A., consultando los hechos y ofreciendo la posibilidad de usar el correo electrónico corporativo que tiene cada trabajador asignado. La representante de RRHH respondió que ello no era posible, dado que el cliente tenía habilitado el envío a través del teléfono personal.

La denunciante indica que la sede en Madrid también está trabajando en la misma campaña con ***EMPRESA.2**, por lo que presupone que se ha actuado de la misma manera con los trabajadores de aquel centro de trabajo.

Se cuenta con la siguiente documentación:

a) Escrito de denuncia ante la AEPD, con fecha de 15/03/2024.
b) Captura de pantalla del mensaje recibido en el teléfono móvil de un trabajador por parte de ***EMPRESA.2 (***EMPRESA.3**) informando de la contraseña.
c) Correos electrónicos enviados por las secciones sindicales y MAJOREL SP SOLUTIONS, S.A. sobre la cesión de datos de los trabajadores a ***EMPRESA.2,** durante febrero de 2024.
d) Contrato entre MAJOREL SP SOLUTIONS, S.A. y ***EMPRESA.2** para la prestación de servicios de atención al cliente de esta, con fecha de 6/02/2024.

SEGUNDO: Como consecuencia de los hechos conocidos, con fecha 13/05/2024, la Presidencia de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

TERCERO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE)

2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VIII, de la LOPDGDD.

Como consecuencia de las actuaciones realizadas, se ha tenido conocimiento de los siguientes extremos:

Como consecuencia de denuncia, esta Agencia ha tenido conocimiento de la existencia de una posible infracción de la normativa de protección de datos en relación con la cesión de datos personales de los representantes y empleados de la empresa MAJOREL SP SOLUTIONS, S.A., (que opera con la marca ******EMPRESA.4***) a la mercantil ******EMPRESA.2*** (nombre comercial, ******EMPRESA.2***), para la ejecución de un contrato de arrendamiento de servicios suscrito entre ambas.

El objeto de dicho contrato es la colaboración entre ******EMPRESA.3*** (China) ***y ***EMPRESA.2*** con la filial autorizada MAJOREL SP SOLUTIONS, S.A***.*** para la realización de actividades de atención al cliente en el mercado español, así como para regular las relaciones y obligaciones entre las partes derivadas de la prestación de los servicios de *Contact Center*.

Según consta en la denuncia, el mencionado contrato no incluía información sobre el consentimiento para transferir datos personales de los trabajadores a una empresa internacional.

La parte denunciante indica que algunos trabajadores de MAJOREL SP SOLUTIONS, S.A***,*** han recibido mensajes de ******EMPRESA.2*** con los datos de acceso a los aplicativos de dicha empresa, deduciendo que ha habido una cesión de los números de teléfono de los trabajadores.

Teniendo en cuenta la relevancia de la información, resulta necesario por esta Agencia conocer en profundidad los hechos descritos y los tratamientos llevados a cabo para, en su caso, determinar las consecuencias que de ellos pueden derivarse para los derechos y libertades de las personas.

En fecha 16/05/2025 se realizó requerimiento de información a la entidad MAJOREL SP SOLUTIONS, S.A.. en relación con los siguientes extremos:

> 1.- Base de legitimación para la cesión internacional de los datos de los representantes de los trabajadores y de los trabajadores de MAJOREL SP SOLUTIONS, S.A., a ******EMPRESA.2***.
> 2.- Categorías de datos y datos cedidos de los representantes de los trabajadores y de los trabajadores de MAJOREL SP SOLUTIONS, S.A.
> 3.-Si entre los datos cedidos se encuentra el teléfono personal de los trabajadores, se deberá justificar.
> 4- Actuaciones que por parte de MAJOREL SP SOLUTIONS, S.A. se han realizado para la comunicación de los datos de los trabajadores.
> 5.- Número de trabajadores afectados, información que sobre la cesión de los datos se ha facilitado a los representantes de los trabajadores y a los trabajadores.
> 6.- Si para la realización de la cesión de los datos de los trabajadores se ha pedido informe al Delegado de Protección de Datos de MAJOREL SP

SOLUTIONS, S.A. (Se deberá aportar los informes del Delegado de Protección de Datos, en su caso).
7.- Si con carácter previo a esa cesión se realizó un análisis de riesgo o una evaluación de impacto en materia de protección de datos (Se deberá aportar dicho análisis o evaluación, en su caso).
8.- Medidas que en materia de protección de datos se hayan previsto para proteger la cesión de los datos de los trabajadores.
9.- Cualquier otra información que estime procedente.

En fecha 30/05/2025, MAJOREL SP SOLUTIONS, S.A. presentó escrito de contestación a dicho requerimiento de información, en el que entre otros aspectos manifiesta:

1. *"Aclaración sobre la relación contractual con* ******EMPRESA.2***.
   En su requerimiento de información, la AEPD expone que existe una cesión de datos de los representantes y empleados de ******EMPRESA.5*** *a la mercantil* ******EMPRESA.2,*** *que denomina* ******EMPRESA.2***. *Sin embargo, actualmente* ******EMPRESA.5*** *tiene una relación contractual directamente con* ******EMPRESA.3*** ******EMPRESA.6***, *empresa que ostenta la marca* ******EMPRESA.2***. *La empresa que hacen mención era una filial del antiguo grupo empresarial que formaba* ******EMPRESA.5*** *ignorándose qué relación puede tener en los hechos de los que se trata*.

2. *Antecedentes de hechos*
   ******EMPRESA.2*** *cuenta con una herramienta denominada* ******EMPRESA.7*** *para acceder y trabajar en sus sistemas, ya que es a través de esta aplicación por donde se crea un token que permite la doble autenticación del agente de* ******EMPRESA.5.*** *De esta forma, solo podrán acceder a esta aplicación aquéllos que hayan sido registrados previamente en la herramienta.*
   Para recibir este token, debemos introducir una serie de datos personales de empleados entre los que se incluye su teléfono móvil, que es donde reciben las credenciales a través de un SMS. El cliente ha insistido que no es posible enviarles un correo electrónico corporativo como medio alternativo, incidiendo en la importancia de disponer de un teléfono correcto, ya que si no el agente no puede hacer el onboarding correcto y crear un usuario.

   *Los datos solicitados por la herramienta de ***EMPRESA.3 son los siguientes:*
   (se adjunta imagen de dos líneas de hoja Excel)

   Al no tener todos los agentes teléfonos móviles profesionales, como solución temporal se utilizaron los teléfonos personales de nuestros agentes.

   Esta cuestión fue discutida hace unos meses y se solicitó la opinión del Delegado de Protección de Datos (en adelante, "DPO") y del Director Legal de ******EMPRESA.5***, *determinando que el uso de teléfonos personales para fines profesionales es contrario a la normativa de protección de datos (adjuntamos como ANEXO 1).*

   Por ello, estamos en un proceso de transición, de tal forma que en el servicio de ******EMPRESA.2*** *se han comprado móviles y SIMs para todas las nuevas*

incorporaciones al equipo desde el 15 de julio pasado. Respecto de las incorporaciones anteriores a esa fecha, estamos retirando todos los teléfonos personales para sustituirlos por teléfonos corporativos y esperamos finalizar este proceso en las próximas semanas.
*Actualmente, de las 364 personas activas del servicio de ***EMPRESA.2, 203 personas tienen asociado el teléfono personal.*

3. *Base de legitimación, categorías de datos e información a los empleados*
*La base de legitimación para la cesión de datos entre *****EMPRESA.5 y ***EMPRESA.2** es la necesidad para la ejecución de un contrato en el que el interesado es parte de la ejecución de una obligación contractual (art.6.1. b) del RGPD).*

*Esta base de legitimación requiere que, efectivamente, este tratamiento sea necesario para la ejecución de las obligaciones contractuales existentes entre el agente y *****EMPRESA.5.** Si bien no se encuentra estipulado en el contrato la necesidad de ceder estos datos a la herramienta del cliente, esta obligación contractual deberá considerarse en el contexto más amplio del acuerdo celebrado (1). Podemos determinar que la cesión de los datos personales anteriormente mencionados es estrictamente necesario para la ejecución del mismo, ya que el cliente debe proteger sus sistemas de accesos ilegítimos y, para poder respetar nosotros el servicio cumpliendo con los estándares de seguridad del cliente, es necesario cederle los datos necesarios para poder identificar de manera inequívoca a los agentes. De otra forma, el empleado no podría prestar los servicios para los que fue contratado ya que, si no se realiza está doble autenticación, los datos personales del cliente a los que accede están desprotegidos.*

*Asimismo, los datos personales que se ceden a *****EMPRESA.2** tienen la única finalidad de crearle su usuario en la herramienta del cliente, sin utilizarse para ningún otro propósito distinto, en línea con el principio de limitación de la finalidad del art.5.1. b) del RGPD. Los agentes son conscientes de la creación de estos usuarios ya que acceden a la herramienta del cliente para poder prestar el servicio, pues le permiten entrar en los sistemas del cliente a través de una VPN.*
*Es por ello que éstos tienen unas expectativas razonables de que, para poderles crear dichos usuarios, es necesario que ***EMPRESA.5 ceda sus datos personales. De otra manera, sería imposible poder tener trazabilidad de cada usuario y mantener un nivel adecuado de seguridad, evitando el fraude o cualquier otro incidente de seguridad.*
*Por otro lado, en nuestra Política de Privacidad de empleados informamos sobre este tipo de tratamiento con su correspondiente base de legitimación informando sobre el tratamiento de sus datos para la correcta gestión del alta de un usuario en un software de un proveedor para permitir que estos les den acceso a sus herramientas mientras trabaja para nosotros (incorporamos capturas de la Política de Privacidad, así como adjuntamos ANEXO 2 la política de privacidad de ***EMPRESA.5). Por tanto, esta cesión de datos siempre ha sido informada y transparente, conforme al principio de licitud, lealtad y trasparencia del art.5.1.a) del RGPD.*

*Las categorías de datos que cedemos a *****EMPRESA.2** son los siguientes:*

- *Nombre.*
- *DNI.*
- *Nombre.*
- *Sexo.*
- *Código de país del teléfono.*
- *Número de teléfono móvil.*
- *Fecha de incorporación al servicio (fecha efectiva).*
- *Nacionalidad (no se requiere documento de identidad)*
- *Provincia/continente (no se requiere documento de identidad)*
-

Todos estos datos están enfocados a la hora de crear el usuario, así como para demostrar la identidad en caso de que existan dudas o recuperar el usuario en caso de un incidente técnico.
No obstante lo anterior, como ya hemos indicado, tras el informe de nuestro DPO estamos trabajando para sustituir los teléfonos personales por profesionales lo antes posible teniendo en cuenta las circunstancias técnicas existentes.

4. *<u>Medidas aplicadas para la transferencia internacional de datos</u>*
   *La herramienta *****EMPRESA.7** es propiedad de *****EMPRESA.2** y se gestiona principalmente en China, un país fuera del Espacio Económico Europeo (EEE). Los datos recopilados se utilizan para acceder a un entorno seguro que permite a *****EMPRESA.5** cumplir con sus obligaciones contractuales, pues el responsable del tratamiento debe adoptar las medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos de la normativa.*
   ******EMPRESA.5** llevó a cabo una evaluación de protección de terceros países (China), así como una evaluación del impacto de la transferencia de España a China, determinando la necesidad de implementar una serie de medidas adicionales para garantizar que dicha transferencia cumpla con la normativa (adjunta como ANEXO 3*).

5. *<u>Medidas adoptadas o en proceso de adaptación para solucionar</u>*
   *Teniendo en cuenta todo lo anterior, entendemos que la cesión de datos de nuestros empleados a *****EMPRESA.2** para la creación de un usuario en su herramienta por motivo de seguridad es legítimo, ya que es necesario para la ejecución del contrato, ha sido informado y existía expectativas razonables por parte de los empleados de dicha. No obstante, lo anterior, el uso de teléfonos personales para esta finalidad no se encontraría dentro del supuesto anterior.*

   Por todo lo anterior, propone varias medidas mitigadoras:

   1. Informar a todos los empleados de una nueva política que incluya de forma más específica la posible cesión de datos a los clientes.
   *2. Realizar una comunicación específica a los agentes del servicio de ***EMPRESA.2 sobre dicha cesión de datos.*
   3. Cambiar los números de teléfonos personales de la herramienta del cliente por profesionales."

CUARTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad MAJOREL SP SOLUTIONS, S.A. es una empresa constituida en el año 1998 y con un volumen de negocios de 201.821.516€ en el año 2023.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Presidencia de la Agencia Española de Protección de Datos.

II
Procedimiento

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos".*

De acuerdo con el artículo 64 de la LOPDGDD, y teniendo en cuenta las características de la presunta infracción cometida, se inicia un procedimiento sancionador.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones, de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

III
Cuestiones previas

El artículo 4.1) del RGPD, define «*dato personal*» como: "*toda información sobre una persona física identificada o identificable («el interesado»*); *se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*

El artículo 4.2) del RGPD, define «*tratamiento*» como: "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*."

El artículo 4.7) del RGPD, define al «*responsable del tratamiento*» o «*responsable*» como: "*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros*". A su vez el artículo 4.8) del RGPD determina al «*encargado del tratamiento*» o «*encargado*» *como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento."*

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que MAJOREL SP SOLUTIONS, S.A. realiza, entre otros tratamientos, la recogida y conservación de datos personales de sus empleados como: DNI, nombre, sexo, código de País del teléfono, número de teléfono móvil, fecha de incorporación al servicio, nacionalidad, provincia y fecha de nacimiento.

MAJOREL SP SOLUTIONS, S.A. realiza esta actividad en su condición de encargado del tratamiento, dado que es quien recoge los datos de sus empleados, con la finalidad de crearles su usuario en la herramienta informática de su cliente ******EMPRESA.2,*** todo ello en virtud del artículo 4.8 del RGPD.

IV
Obligación incumplida. Artículo 6 RGPD

El artículo 6 del RGPD establece:

"1. El tratamiento solo será licito si se cumple al menos una de las siguientes condiciones:

> *b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales: "*

El fundamento jurídico para el tratamiento en virtud del artículo 6, apartado 1, letra b), debe interpretarse en el contexto del RGPD en su conjunto, de los objetivos establecidos en el artículo 1 y en paralelo con el deber de los responsables del tratamiento, de tratar los datos personales de conformidad con los principios que en materia de protección de datos establece el artículo 5 del RGPD. Ello exige tratar los datos personales de un modo leal y transparente y en consonancia con las obligaciones de limitación de la finalidad y minimización de los datos. El artículo 5.1.a) del RGPD establece que los datos personales deben ser tratados de manera *lícita, leal y transparente* en relación con el interesado. El principio de lealtad incluye, entre

otros, el reconocimiento de unas expectativas razonables de los interesados, la consideración de las posibles consecuencias adversas que el tratamiento pueda tener sobre estos y la consideración de la relación y los posibles efectos del desequilibrio entre estos y el responsable del tratamiento.

Respecto al ámbito de aplicación del artículo 6.1.b) del RGPD este se aplica cuando se cumpla cualquiera de las dos condiciones siguientes:

- El tratamiento en cuestión debe ser objetivamente necesario para la ejecución del contrato con el interesado.
- O el tratamiento debe ser objetivamente necesario para la aplicación, a petición de este, de medidas precontractuales.

La necesidad del tratamiento es un requisito previo en ambos supuestos del artículo 6.1.b) del RGPD. Es importante señalar desde el inicio que el concepto de *necesario para la ejecución de un contrato* no consiste en una mera valoración de lo que se permite en las cláusulas del contrato o de los términos en que estas se encuentran redactadas. El concepto de necesidad tiene un significado independiente en el Derecho de la Unión y debe reflejar los objetivos del Derecho en materia de protección de datos. Por tanto, requiere también que se tengan en cuenta el derecho fundamental a la privacidad y a la protección de los datos de carácter personal, así como los requisitos de los principios de protección de datos, en especial, el principio de lealtad.

Es necesario también identificar la finalidad del tratamiento, y, en el contexto de las relaciones contractuales, este tratamiento puede responder a diversos fines. Estos fines deben especificarse y comunicarse de manera clara al interesado, respetando así las obligaciones de limitación de la finalidad y transparencia que debe cumplir el responsable del tratamiento. Al evaluar qué es necesario, debe realizarse una valoración combinada y basada en los hechos del tratamiento para el objetivo que se persigue, evaluando si resulta menos intrusivo que otras opciones disponibles para conseguir el mismo objetivo. Si existen otras alternativas realistas y menos intrusivas, el tratamiento no es necesario.

Por tanto, el artículo 6.1.b) del RGPD, no cubre los tratamientos que resulten útiles pero no sean objetivamente necesarios para ejecutar el servicio objeto del contrato o para aplicar las medidas precontractuales pertinentes a petición del interesado, incluso si resultan necesarios para los demás fines comerciales del responsable del tratamiento.

En el presente caso, entre las categorías de datos que MAJOREL SP SOLUTIONS, S.A. cedió a ******EMPRESA.2***, se encuentra el teléfono móvil personal de los trabajadores, a fin de *crear el usuario, así como para demostrar la identidad en caso de que existan dudas o recuperar el usuario en caso de un incidente técnico.*

El principio de ajenidad en los medios obliga a la empresa a dotar a la persona trabajadora de los medios necesarios para la ejecución de la relación laboral (art. 1.1 Estatuto de los Trabajadores). El uso del teléfono personal no puede considerarse necesario para la ejecución de la relación laboral, y el consentimiento no es una base válida si no se le ofrece al trabajador una vía alternativa que no implique el tratamiento de sus datos personales (Guidelines 2/2017 del Comité Europeo de Protección de Datos).

Esta Agencia ya indicó en varias de sus resoluciones, que es ilegal utilizar el teléfono móvil personal como doble factor de autenticación (Resolución de 3 de enero de 2023), y en términos generales ha indicado que su uso no es posible con fines laborales (Resolución de 10 de octubre de 2023).

La Audiencia Nacional también ha indicado la ilegalidad de esta práctica, haciendo expresa mención del artículo 19.7 del *III Convenio Colectivo Estatal del Sector de Contact Center.*

En este sentido, la Sentencia de la Audiencia Nacional, Sala de lo Social, Nº Resolución 14/2024 de fecha 05/02/2024, (Roj: SAN 487/2024 – ECLI:ES:AN2024:847), señala en su Fundamento de Derecho noveno:
"Finalmente queda por resolver la última de las pretensiones del suplico relativa a que Se declare nulo el contenido de la cláusula novena del acuerdo individual de teletrabajo en el sentido que el trabajador no debe facilitar a la empresa su número de teléfono móvil para la recepción de SMS y/o para acceder a aplicaciones que permiten confirmar la identidad, todo ello de conformidad con lo establecido en el art. 19.7de la norma convencional.
En dicha cláusula del acuerdo de trabajo a distancia se establece lo siguiente:
Por motivos de ciberseguridad, tanto la Compañía y DXC como sus clientes están desplegando de forma progresiva métodos de autentificación y acceso a sistemas o aplicaciones necesarias para la prestación de los servicios. Por ello, la Compañía y DXC puede solicitar a la persona trabajadora, puntualmente, su número de teléfono móvil para la recepción de mensajes de tipo SMS y/o para acceder a aplicaciones que permiten confirmar la identidad, únicamente durante el horario de trabajo establecido. El tratamiento del dato de número teléfono móvil se limitará a la finalidad de verificar la identidad de la Persona Trabajadora durante el acceso a sistemas y aplicaciones, estando este tratamiento amparado en el interés legítimo de la Compañía y DXC en garantizar la seguridad de la información y los sistemas.

Sin duda la Sala reconoce que uno de los procedimientos más difundidos para garantizar la seguridad de las comunicaciones informáticas consiste en el empleo de métodos de autentificación a través de mensajes SMS que remiten un código que el destinatario debe emplear para acceder a determinadas aplicaciones.
El empleo de estos mecanismos para garantizar la identificación de los que acceden a tales aplicaciones no lo cuestionamos, lo que sí resulta controvertido es que los mensajes SMS se remitan al teléfono móvil personal de cada trabajador por cuanto con ello se le impone el empleo para el trabajo de sus personales herramientas y dispositivos.
El art. 19.7 del convenio establece que Las empresas no podrán utilizar herramientas, aplicaciones o dispositivos de las personas trabajadoras que no sean facilitadas por la propia empresa. En el caso de que fuera necesario un sistema de doble factor de autenticación, la empresa deberá facilitar las herramientas y medios necesarios para su uso. Como caso excepcional y exclusivamente para esta finalidad, si la persona trabajadora rechaza la herramienta facilitada por la empresa, podrá dar su consentimiento al uso de dispositivos o herramientas de su propiedad.
De la norma convencional se deduce que los negociadores acuerdan prohibir el empleo de aplicaciones y dispositivos del trabajador y que de ser necesario usar un doble factor de autentificación, lo que ocurre con la emisión de mensajes SMS que

remiten un código para acceder a las aplicaciones, el empresario será quien debe facilitar las herramientas y medios precisos.
Esta previsión convencional se incumple con la cláusula contenida en los acuerdos individuales de trabajo a distancia, que como puede apreciarse, impone al trabajador el uso para la autentificación de su personal teléfono.
Procede que estimemos también esta pretensión."

De las manifestaciones de la parte reclamada se desprende la existencia de una relación contractual entre MAJOREL SP SOLUTIONS, S.A. y ******EMPRESA.2***, quien cuenta con su herramienta informática ******EMPRESA.7*** para acceder y trabajar en sus sistemas, y es a través de esta aplicación por la que se crea un token que permite la doble autenticación del agente de MAJOREL SP SOLUTIONS, S.A., a través del envío de un SMS al teléfono móvil personal de dicho agente, lo que supondría una cesión ilícita de datos.
Actualmente, de las 364 personas activas del servicio de ******EMPRESA.2***, 203 personas tienen asociado su teléfono móvil personal.

En el presente caso, la entidad MAJOREL SP SOLUTIONS, S.A. habría comunicado a la empresa ******EMPRESA.2***, los números de teléfono personales de sus trabajadores, junto con otros datos identificativos, con la finalidad de crear usuarios de acceso en las herramientas informáticas de dicha empresa. La propia entidad reconoce que, ante la inexistencia de terminales corporativos, se decidió de forma temporal utilizar los teléfonos personales de los empleados para recibir los códigos de autenticación necesarios para acceder a los sistemas de ******EMPRESA.2***.
Dicha comunicación de datos personales no puede considerarse amparada en la base jurídica del artículo 6.1.b) del RGPD (ejecución de un contrato en el que el interesado sea parte), tal como sostiene la parte reclamada. La ejecución del contrato laboral no exige ni justifica la cesión del número de teléfono personal del trabajador a un tercero extranjero. Este dato, perteneciente a la esfera privada del empleado, no resulta necesario ni proporcional para el cumplimiento de las obligaciones derivadas de la relación laboral, máxime cuando la propia entidad reconoce que se trató de una medida provisional adoptada por motivos organizativos internos.

Además, consta acreditado que el Delegado de Protección de Datos de MAJOREL SP SOLUTIONS, S.A. emitió un informe advirtiendo expresamente que el uso de teléfonos personales para fines profesionales era contrario a la normativa de protección de datos, lo que evidencia que la entidad era plenamente consciente de la falta de licitud de dicho tratamiento y, pese a ello, lo mantuvo afectando a más de doscientos trabajadores.

La posibilidad de que el empleador se sirva de los terminales y líneas de telefonía móvil del trabajador con fines laborales requiere que dicha utilización hubiera sido elegida voluntaria y libremente por el titular, después de haber recibido la información prevista sobre el tratamiento de sus datos personales y sobre la posibilidad de revocar el consentimiento prestado, en cualquier momento y sin consecuencias perjudiciales. Esa manifestación de voluntad expresa podría entenderse libre, entre otras circunstancias, si la empresa hubiera dispuesto y ofrecido previamente una opción alternativa. En todo caso, además, el empleador y responsable del tratamiento de los datos personales deberá garantizar que las aplicaciones corporativas no accederán a

los datos privados de sus empleados y que existe una separación técnica entre los usos laboral y personal del teléfono móvil de los trabajadores.

Ninguna de las circunstancias expresadas concurre en el presente supuesto.

En consecuencia, la cesión de datos personales sin consentimiento ni base jurídica adecuada constituiría un tratamiento ilícito, vulnerando lo dispuesto en el artículo 6.1 del RGPD. MAJOREL SP SOLUTIONS, S.A. habría actuado como responsable del tratamiento al decidir la comunicación de los datos de sus empleados a un tercero, sin que concurriera ninguna de las condiciones de licitud previstas en el RGPD.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a MAJOREL SP SOLUTIONS, S.A., por vulneración del artículo transcrito anteriormente.

V

Tipificación de la infracción del artículo 6.1.b) del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, que se sancionará, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:
"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:
b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679."

VI

Propuesta de sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.
2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:
a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Por su parte, el artículo 76 *"Sanciones y medidas correctivas"* de la LOPDGDD dispone:
"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado".

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa, además de la adopción de medidas, si procede.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de MAJOREL SP SOLUTIONS, S.A. en 201.821.516€ para el año 2023.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

Con carácter previo, se estima que concurren las circunstancias siguientes:

- La **naturaleza, gravedad y duración de la infracción**, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (artículo 83.2, letra a), del RGPD): de los 364 trabajadores de MAJOREL SP SOLUTIONS, S.A. activas para dar servicio a ******EMPRESA.2***, 203 trabajadores tienen asociado su teléfono móvil personal, al menos desde 6/02/2024, fecha de firma del contrato, hasta 30/05/2025 fecha de respuesta a esta Agencia, por la parte reclamada.

- **Intencionalidad/ Negligencia en la infracción** (artículo 83.2, letra b), del RGPD): no se atendió debidamente al requerimiento hecho por las secciones sindicales~~,~~ –así como, se desprende también que desde el 9/04/2024, fecha de respuesta del DPD, la parte reclamada conocería la irregularidad y no la habría evitado al menos hasta su respuesta a esta Agencia el 30/05/2025~~.~~

- Las **categorías de los datos de carácter personal** afectados por la infracción (artículo 83.2, letra g), del RGPD): los datos de los trabajadores que se cedieron a ******EMPRESA.2*** fueron 9 tipos, a saber: DNI, nombre, sexo, código de País del teléfono, número de teléfono móvil, fecha de incorporación al servicio, nacionalidad, provincia y fecha de nacimiento.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 6.1.b) del RGPD, permite fijar inicialmente una sanción de multa administrativa de **80.000€** (**OCHENTA MIL EUROS).**

VII

Medidas correctivas

De confirmarse la infracción, la resolución que se dicte podrá establecer las medidas correctivas que la entidad infractora deberá adoptar para poner fin al incumplimiento de la legislación de protección de datos personales, en este caso del Artículo 6.1.b) del RGPD, de acuerdo con lo establecido en el citado artículo 58.2.d) del RGPD, según el cual cada autoridad de control podrá "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…"*
Así, se podrá requerir a la entidad responsable para que adecúe su actuación a la normativa de protección de datos personales, con el alcance expresado en los anteriores Fundamentos de Derecho.

En el presente acto se establece cuál es la presunta infracción cometida y los hechos que podrían dar lugar a esa posible vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.
MAJOREL SP SOLUTIONS, S.A. manifiesta que está en proceso para *dotar de teléfonos y SIMs profesionales a todas las personas activas del servicio de* ******EMPRESA.2***, así como propone varias medidas mitigadoras de esta situación:

- Evitar el uso de datos personales, como el número de teléfono personal, con fines laborales.

No obstante, en este caso, con independencia de lo anterior, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, en la resolución que se adopte se podrá requerir a MAJOREL SP SOLUTIONS, S.A.. para que, en el plazo máximo de 3 meses, a contar desde la fecha de ejecutividad de la resolución finalizadora de este procedimiento, adopte las medidas siguientes:

- Cesar en el tratamiento de datos: no utilizar los teléfonos móviles de los empleados de MAJOREL SP SOLUTIONS, S.A. que presten servicio a ******EMPRESA.2***, como terminales de acceso a la aplicación informática de esta última.

La imposición de estas medidas es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución del presente procedimiento sancionador podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Asimismo, se recuerda que ni el reconocimiento de la infracción cometida ni, en su caso, el pago voluntario de las cuantías propuestas, eximen de la obligación de adoptar las medidas pertinentes para que cese la conducta o se corrijan los efectos de la infracción cometida y la de acreditar ante esta AEPD el cumplimiento de esa obligación.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Presidencia de la Agencia Española de Protección de Datos,
SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a ***MAJOREL SP SOLUTIONS, S.A.***, con NIF ***A82112665***, por la presunta infracción del Artículo 6.1.b) del RGPD, tipificada en el artículo 83.5 del RGPD.

SEGUNDO: NOMBRAR como instructora a ***R.R.R.*** y, como secretaria, a ***S.S.S.*** indicando que podrán ser recusados, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente, a efectos probatorios, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de multa administrativa de 80.000,00 euros, sin perjuicio de lo que resulte de la instrucción.

QUINTO: NOTIFICAR el presente acuerdo a ***MAJOREL SP SOLUTIONS, S.A.***, con NIF ***A82112665***, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en **64.000,00** euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en **64.000,00** euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento

de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en **48.000,00 euros**.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente **(64.000,00** euros o **48.000,00 euros**), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

En cumplimiento de los artículos 14, 41 y 43 de la LPACAP, se advierte de que, en lo sucesivo, las notificaciones que se le remitan se realizarán exclusivamente de forma electrónica, a través de la Dirección Electrónica Habilitada única (dehu.redsara.es) y de la Sede electrónica (sedeaepd.gob.es), y que, de no acceder a ellas, se hará constar su rechazo en el expediente, dando por efectuado el trámite y siguiéndose el procedimiento. Se le informa que puede identificar ante esta Agencia una dirección de correo electrónico para recibir el aviso de puesta a disposición de las notificaciones y que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

1479-010725

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos

>>

SEGUNDO**:** En fecha 19 de noviembre de 2025, ***MAJOREL SP SOLUTIONS, S.A.*** ha procedido al pago de la sanción en la cuantía de **48.000,00 euros** haciendo uso de las dos reducciones previstas en el acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad en relación con los hechos a los que se refiere el acuerdo de inicio y su calificación jurídica.

TERCERO: En el acuerdo de inicio transcrito anteriormente se señalaba que, de confirmarse la infracción, podría acordarse imponer al responsable la adopción de

medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *"ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".*

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en el acuerdo de inicio.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para resolver este procedimiento la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí.

Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

III

Pago voluntario y reconocimiento de responsabilidad

De conformidad con lo dispuesto en el citado artículo 85 de la LPACAP, en el acuerdo de inicio notificado se informaba sobre la posibilidad de reconocer la responsabilidad y de realizar el pago voluntario de la sanción propuesta, lo que supondría dos reducciones acumulables de un 20% cada una. Con la aplicación de estas dos reducciones, la sanción quedaría establecida en **48.000,00 euros** y su pago implicaría la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

Tras la notificación del citado acuerdo de inicio, ***MAJOREL SP SOLUTIONS, S.A.*** ha procedido al reconocimiento de la responsabilidad y al pago voluntario de la sanción, acogiéndose a las dos reducciones previstas. De conformidad con el apartado 3 del artículo 85 LPACAP, la efectividad de las citadas reducciones estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

Debe tenerse en cuenta que, de acuerdo con los preceptos de la LPACAP, así como de la jurisprudencia del Tribunal Supremo en esta materia, el ejercicio del pago voluntario por el presunto responsable no exime a la administración de la obligación de resolver y notificar todos los procedimientos, cualquiera que sea su forma de iniciación. De igual forma, el artículo 88 de la citada norma establece que la resolución que ponga fin al procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones, la Presidencia de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la comisión de las infracciones y CONFIRMAR las sanciones determinadas en la parte dispositiva del acuerdo de inicio transcrito en la presente resolución.

La suma de las citadas cuantías arroja una cantidad total de **80.000,00 euros.**

Tras haber procedido ***MAJOREL SP SOLUTIONS, S.A.*** al pronto pago y reconocimiento de responsabilidad, se procede, en virtud del artículo 85 de la LPACAP, a la reducción de un 40% del total mencionado, lo cual supone la cantidad definitiva de **48.000,00 euros**.

La efectividad de las citadas reducciones está condicionada, en todo caso, al desistimiento o renuncia de cualquier acción o recurso en vía administrativa.

SEGUNDO: DECLARAR la terminación del procedimiento **EXP202406971**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

TERCERO: ORDENAR a ***MAJOREL SP SOLUTIONS, S.A.*** para que en el plazo de 3 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del acuerdo de inicio transcrito en la presente resolución.

CUARTO: NOTIFICAR la presente resolución a ***MAJOREL SP SOLUTIONS, S.A.***.

QUINTO: De acuerdo con lo previsto en el artículo 85 de la LPACAP que condiciona la reducción por pago voluntario y reconocimiento de la responsabilidad al desistimiento o renuncia de cualquier acción o recurso en vía administrativa, la presente resolución será firme en vía administrativa y plenamente ejecutiva a partir de su notificación.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará una vez la resolución 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, los interesados podrán interponer 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.

No obstante, conforme a lo previsto en el artículo 90.3.a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeaepd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

1259-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos