

- **Expediente N.º: PS/00178/2022**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: La Dirección General de la Policía, Comisaría de Moncloa-Aravaca (en lo sucesivo Policía Nacional), con fecha 16/11/2020 interpuso reclamación ante la Agencia Española de Protección de Datos contra la entidad MUXERS CONCEPT, S.L., con NIF B87345369 (en adelante, la parte reclamada o MUXERS). Los motivos en que basa la reclamación son los siguientes:

La Policía Nacional da cuenta de la denuncia formulada ante el Grupo de Policía Judicial por cinco trabajadores de un restaurante perteneciente a la parte reclamada, por el *“hallazgo de un sistema de grabación de audio en el vestuario de la empresa”*, oculto en un falso techo; así como de las diligencias instruidas con ese motivo.

Aporta copia de las denuncias reseñadas, en las que los denunciantes declaran haber encontrado en el aseo de empleados, donde también se encuentran sus taquillas, una supuesta cámara de videovigilancia y grabadora de sonido, enchufada y en condiciones de uso (en tres de las cinco denuncias se alude únicamente a un micrófono). Manifiestan, asimismo, que no fueron informados sobre la instalación de estos dispositivos.

La Policía Nacional aporta también copia de un acta, de 27/10/2020, extendida para proceder a la intervención de un *“Micrófono con numeración Air Space AA003”*, y fotografías en las que se ve la localización de este dispositivo en un falso techo. Según consta en este Acta, la persona interesada que presencia la intervención de la Policía Nacional manifiesta *“que el micrófono intervenido es propiedad de la empresa Muxers Concept, S.L., CIF...”*.

Por otra parte, con fecha 20/04/2021, se recibió reclamación presentada por **A.A.A.** (en adelante, la parte reclamante), también dirigida contra la entidad MUXERS, en la que manifiesta que el día 27/10/2020, en compañía de otros compañeros, descubrieron en su centro de trabajo (el mismo al que se refiere la reclamación del a Policía Nacional) *“la colocación de cámaras de grabación de audio/video en los aseos correspondientes a los vestuarios de las trabajadoras”*.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de la reclamación recibida de la Policía Nacional a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos

previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) mediante notificación electrónica, no fue recogido por el responsable, dentro del plazo de puesta a disposición, entendiéndose rechazada conforme a lo previsto en el art. 43.2 de la LPACAP en fecha 20/12/2020, como consta en el certificado que obra en el expediente.

Aunque la notificación se practicó válidamente por medios electrónicos, dándose por efectuado el trámite conforme a lo dispuesto en el artículo 41.5 de la LPACAP, a título informativo se envió una copia por correo postal que fue notificada fehacientemente en fecha 18/01/2021. En dicha notificación, se le recordaba su obligación de relacionarse electrónicamente con la Administración, y se le informaban de los medios de acceso a dichas notificaciones, reiterando que, en lo sucesivo, se le notificaría exclusivamente por medios electrónicos.

Con fecha 17/02/2021, se recibe en esta Agencia escrito de respuesta facilitado por la parte reclamada, en el que manifiesta lo siguiente:

El sistema, que fue instalado por la entidad Teknometric Biometric Solutions and New Technologies, S.L. (Teknometric) en fecha 20/06/2018, dispone de 22 cámaras dentro del local, 2 cámaras exteriores en fachada, 1 equipo de grabación y 4 micrófonos de audio preamplificados, sin que existiera ningún dispositivo en el vestuario ni en los baños.

Sobre la existencia de un contrato por el que encargue a un tercero la visualización y/o audición de las imágenes y/o audios, informa que existe contrato con la compañía *“Stop Alarma puesto que la instalación corresponde al sistema de videovigilancia”*. Se adjunta contrato y certificado de conexión a central de alarmas y certificado de video verificación con esa compañía.

En relación con la finalidad de la instalación de equipos de videovigilancia, señala que dicha finalidad es *“el control de acceso de personas, mercancías... seguridad de los bienes y las personas”*. A este respecto, advierte que se realizó comunicación escrita a los trabajadores desde la apertura y constan las cartas firmadas de conformidad por cada trabajador sobre la colocación, el carácter de las mismas y su ubicación.

Sobre las causas que motivaron la reclamación, añade la parte reclamada que el enrarecimiento de la relación laboral causado por la reducción de jornada de los trabajadores y no haber cobrado las cantidades debidas por el ERTE parcial, motivó que las trabajadoras levantaran el falso techo y arrastraran el micro del office (donde si hay micrófono) y lo llevaran a la zona de vestuarios, no a los baños, y de ahí toda la controversia.

Adicionalmente, todas las trabajadoras han denunciado penalmente al dueño de la empresa, y han existido despidos con las correspondientes demandas en el Tribunal de lo Social.

Constan denuncias por parte de la empresa contra las citadas trabajadoras por ese

incidente, que provocó el despido de algunas de ellas, entre otras de la encargada que haciendo dejación de sus funciones admitió la entrada de personas ajenas al local y urdió todo un plan con el fin de pedir dinero por todos los medios, como así ha sido.

Se adjuntan las denuncias de la empresa, las cartas de reducción de jornada, que explican las verdaderas razones de este asunto, que no tiene nada que ver con la colocación de cámaras o micros puesto que la empresa nunca los ha colocado y consta en el plano de ubicaciones desde el primer día de apertura del local y la comunicación a las trabajadoras desde agosto de 2018.

Por tanto, según la parte reclamada, difícilmente los trabajadores pueden decir, como dicen que desconocieran la ubicación de los sistemas de seguridad cuando eran conocedores desde el inicio de su existencia, finalidad, ubicación, etc.

Para más señas, el abogado de una de las denunciadas ha pedido a la empresa 35.000 euros por este tema de compensación para no ir a juicio.

Todo en la línea que hemos dicho de presionar a la empresa para indemnizar a las trabajadoras o para readmitirlas.

Con su respuesta aporta la siguiente documentación relevante:

- . Plano de situación de las cámaras y micrófonos (22 cámaras interiores, 2 cámaras exteriores, 1 equipo de grabación, 4 micrófonos de audio preamplificados). Según este plano, elaborado por Teknometric, los micrófonos constan instalados en el acceso al restaurante, en la sala donde están ubicadas las mesas y barra del establecimiento (más de XX mesas de distintas dimensiones -entre y seis puestos- y 12 puestos de barra), en un office y en una estancia de pequeño tamaño cuyo uso no está especificado en el plano.

- . Fotografías de la localización de las cámaras

- . Aporta una fotografía en la que se aprecia la existencia de un cartel informativo de la existencia de las cámaras, ubicado en el interior del local.

- . Aporta factura de la instaladora de las cámaras Teknometric, en la que se detalla el sistema instalado, integrado por 22 cámaras interiores, 2 exteriores, un grabador de videovigilancia y 4 salidas de audio con disco duro, y *“4 micros ocultos preamplificados”*; e informe técnico emitido por esta misma entidad sobre la instalación de estos dispositivos en fecha 20/06/2018. En este informe se indica que MUXERS fue informada *“de la normativa y la legalidad en cuanto al aviso de sus empleados ante la colocación de micrófonos de audio”*.

- . “Certificado video verificación” y “Certificado de conexión a central de alarmas” emitidos por la entidad Stop Alarmas, S.L.U. Este último incluye un apartado denominado “Verificación” en el que constan marcadas las opciones “Secuencial”, “Imagen” y “Bidireccional”. No consta marcada la opción “Audio”.

- . 10 documentos fechados el 20/08/2018, con el rótulo *“Comunicación al*

trabajador de la existencia de cámaras de videovigilancia cuyas imágenes pueden ser utilizadas para control de obligaciones y deberes laborales". A información contenida en estos documentos consta extractada en el Hecho Probado Cuarto.

. Denuncia formulada ante la Policía Nacional por la administradora de la entidad MUXERS, por destrozos ocasionados en el vestuario del personal en fecha 27/10/2020 (*"el techo está roto y los cables de los micrófonos que había en el interior colgando"*). En este documento se recogen las manifestaciones de la denunciante. Entre ellas, las siguientes:

"Que la denunciante manifiesta que son micrófonos, que en el contrato de trabajo viene especificado la grabación de audio y vídeo, y que ellas mismas han firmado".

"Que a las 13:20 se persona otro indicativo de la Policía Nacional los cuales vienen a incautar el micrófono del vestuario quedando todo ello plasmado en un Acta de Intervención de Efectos de la cual entregan copia a la denunciante".

TERCERO: Con fecha 22/02/2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la Policía Nacional.

Igualmente, la reclamación formulada por la parte reclamante fue admitida a trámite en fecha 07/05/2021.

CUARTO: 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 VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

. Se remitió una solicitud de información a la parte reclamada, mediante envío postal dirigido al mismo domicilio en el que se practicó la notificación del traslado reseñado en el Antecedente anterior, sin que en este caso la notificación pudiera practicarse (resultó devuelta con la indicación "desconocido").

. La Policía Nacional, con fecha 03/12/2021, informó a los Servicios de Inspección que el atestado policial de la Comisaria de Moncloa-Aravaca, ha dado lugar a la apertura Diligencias Previas N.º *****DILIGENCIAS.1**, seguidas en el Juzgado de Instrucción N.º **XX** de Madrid.

. Solicitada información al citado Juzgado de Instrucción sobre la posible responsabilidad de la parte reclamada en la instalación de los dispositivos de grabación de audio y vídeo en los vestuarios y aseos de uso por los trabajadores del establecimiento al que se refieren las reclamaciones, no se recibió contestación de dicho juzgado durante el plazo de estas actuaciones de investigación.

Así, se acordó declarar la caducidad de las citadas actuaciones previas de investigación y abrir nuevas actuaciones de investigación, así como incorporar a las mismas la documentación que integra las actuaciones caducadas.

La respuesta del Juzgado de Instrucción se recibió con fecha 26/01/2022, en la que se

informa que de lo actuado hasta el día de la fecha (18/01/2022) en el Procedimiento Abreviado que sigue bajo el número *****DILIGENCIAS.1**, *“no consta determinada la responsabilidad de la entidad MUXERS CONCEPT, S.L.”*.

QUINTO: Con fecha 13/05/2022, por la Subdirección General de Inspección de Datos se accede a la información relativa a la entidad MUXERS en “Axesor” (“Informe monitoriza”). (...).

SEXTO: Con fecha 20/05/2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la entidad MUXERS, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción del artículo 6 del RGPD, tipificada en el artículo 83.5.a) del citado Reglamento; y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD.

En el acuerdo de apertura se determinó que la sanción que pudiera corresponder, atendidas las evidencias existentes en el momento de la apertura y sin perjuicio de lo que resulte de la instrucción, ascendería a un total de 20.000 euros (veinte mil euros).

La notificación de este acuerdo de apertura a la parte reclamada, en la que se concedía plazo para formular alegaciones y proponer prueba, se remitió mediante el Servicio de Notificaciones Electrónicas, si bien la misma no fue recogida por la parte reclamada dentro del plazo de puesta a disposición.

Aunque la notificación se practicó válidamente por medios electrónicos, dándose por efectuado el trámite conforme a lo dispuesto en el artículo 41.5 de la LPACAP, con fecha 09/06/2022 se realizó un nuevo intento de notificación por vía postal, siendo devuelto el envío por dirección incorrecta, a pesar de que el mismo se dirigió al domicilio social de la entidad que consta en el Registro Mercantil.

Asimismo, con fecha 23/06/2022 se publicó en el Boletín Oficial del Estado un anuncio de notificación de la apertura de procedimiento. En dicho anuncio se informa a la parte reclamada sobre la posibilidad de obtener copia del acuerdo de apertura.

SÉPTIMO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la LPACAP y transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la LPACAP -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

1. la entidad MUXERS es responsable del sistema de videovigilancia instalado en el local en el que desarrolla su actividad en fecha 20/06/2018. Se trata de un establecimiento abierto al público dedicado a la restauración.

2. El sistema de videovigilancia reseñado en el Hecho Probado Primero, además de las cámaras de videovigilancia, cuenta con cuatro micrófonos de audio preamplificados, instalados en el acceso al restaurante, en la sala donde están ubicadas las mesas y barra del establecimiento (más de 30 mesas de distintas dimensiones -entre y seis puestos- y 12 puestos de barra), en un office y en una estancia de pequeño tamaño cuyo uso no consta especificado.

Dicho sistema dispone de un grabador de videovigilancia y 4 salidas de audio con disco duro.

3. La finalidad pretendida con la instalación de estos equipos es el control de accesos de personas y mercancías, la seguridad de los bienes y las personas, así como el control de obligaciones y deberes laborales.

4. En el momento de la instalación del sistema de videovigilancia, la entidad MUXERS facilitó a sus trabajadores un documento informativo con el rótulo *“Comunicación al trabajador de la existencia de cámaras de videovigilancia cuyas imágenes pueden ser utilizadas para control de obligaciones y deberes laborales”*. Según estos documentos, la parte reclamada informa al trabajador que lo suscribe como sigue:

“De conformidad con la Ley 5/1999... INFORMA a... (nombre y apellidos del trabajador) de la grabación a través de videocámaras en las instalaciones internas y externas de la mercantil de la que resulta un tratamiento responsabilidad de Muxers Concept, SL en el que quedan almacenados sus datos personales, incluida su imagen y sonido obtenidos, grabados y captados a través de la cámaras y videocámaras, con los siguientes fines:

I. Vigilancia

Vigilancia interior y exterior de las instalaciones de la mercantil..., con la finalidad de dar cumplimiento al operativo de seguridad y para prevenir riesgos que afecten a la seguridad y protección de las personas, locales y bienes patrimoniales así como para denunciar, cuando sea necesario, hechos ante las autoridades competentes o atender requerimientos de las mismas.

II. Calidad y rendimiento laboral

Control de la calidad y rendimiento laboral de los trabajadores así como verificación del cumplimiento por... (nombre y apellidos del trabajador) de sus obligaciones y deberes laborales.

III. Sanciones disciplinarias

Las imágenes y sonido captadas por las cámaras de videovigilancia podrán ser utilizadas para la detección por Muxers... de actos delictivos o faltas laborales recogidas en el convenio

colectivo... como prueba a la hora de sancionar

...los instrumentos técnicos empleados... respetan el derecho a la intimidad, dentro del ejercicio legítimo de la facultad de vigilancia empresarial”.

5. Con motivo de unas denuncias formuladas por trabajadores del restaurante, la Policía Nacional se personó en el establecimiento de MUXERS y levantó acta de fecha 27/10/2020, extendida para proceder a la intervención de un *“Micrófono con numeración Air Space AA003”*. Ese documento incorpora unas fotografías en las que se ve la localización de este dispositivo en un falso techo. Según consta en este Acta, la persona interesada que, en representación de MUXERS, presencia la intervención de la Policía Nacional manifiesta *“que el micrófono intervenido es propiedad de la empresa Muxers Concept, S.L., CIF...”*.

En su respuesta al trámite de traslado de la reclamación, MUXERS manifestó que el micrófono intervenido por la Policía Nacional se encontraba en el office habilitado en el establecimiento.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del 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 Directora 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 registrarán 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

La imagen y la voz son un dato personal

La imagen física y la voz de una persona, a tenor del artículo 4.1 del RGPD, son un dato personal y su protección, por tanto, es objeto de dicho Reglamento. En el artículo 4.2 del RGPD se define el concepto de “tratamiento” de datos personales.

Las imágenes y la voz captadas por un sistema de cámaras o videocámaras son datos de carácter personal, por lo que su tratamiento está sujeto a la normativa de protección de datos.

Es, por tanto, pertinente analizar si el tratamiento de datos personales (imagen y voz de los trabajadores en el establecimiento al que se refieren las reclamaciones, cuya titularidad corresponde a la parte reclamada, y de las personas físicas que acuden como clientes al dicho establecimiento, abierto al público) llevado a cabo a través del

sistema de videovigilancia denunciado es acorde con lo establecido en el RGPD.

III Infracción

El artículo 6.1 del RGPD establece los supuestos que permiten considerar lícito el tratamiento de datos personales.

La implantación permanente de un sistema de cámaras de video por razones de seguridad tiene base legítima en la LOPDGDD, cuya exposición de motivos indica:

“Junto a estos supuestos se recogen otros, tales como la videovigilancia... en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679”.

En cuanto al tratamiento con fines de videovigilancia, el artículo 22 de la LOPDGDD establece que las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Este mismo artículo 22, en su apartado 8, dispone que *“El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica”.*

Sobre la legitimación para la implantación de sistemas de videovigilancia en el ámbito laboral, se tiene en cuenta el Real Decreto Legislativo 1/1995, de 24/03, que aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (LET), cuyo artículo 20.3 señala:

“3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad”.

Entre las medidas de vigilancia y control admitidas se incluye la instalación de cámaras de seguridad, si bien estos sistemas deberán responder siempre al principio de proporcionalidad, es decir, el uso de las videocámaras debe ser proporcional al fin perseguido, esto es garantizar la seguridad y el cumplimiento de las obligaciones y deberes laborales.

El artículo 89 de la LOPDGDD, referido específicamente al *“derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo”* y al tratamiento de datos personales obtenidos con sistemas de cámaras o videocámaras para el ejercicio de funciones de control de los trabajadores, permite que los empleadores puedan tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al

mismo.

En relación con la grabación de sonidos, el citado artículo 89 de la LOPDGDD establece lo siguiente:

“2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley”.

Por otra parte, interesa destacar que, según doctrina del Tribunal Constitucional, la grabación de conversaciones entre trabajadores o entre éstos y clientes no se justifica por la verificación del cumplimiento por el trabajador de sus obligaciones o deberes. En Sentencia de fecha 10/04/2000 (2000/98), dictada en el rec. núm. 4015/1996, se declara lo siguiente:

“En este sentido debe tenerse en cuenta que el poder de dirección del empresario, imprescindible para la buena marcha de la organización productiva y reconocido expresamente en el art. 20 LET, atribuye al empresario, entre otras facultades, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales (art. 20.3 LET). Mas esa facultad ha de producirse en todo caso, como es lógico, dentro del debido respeto a la dignidad del trabajador, como expresamente nos lo recuerda la normativa laboral (arts. 4.2.e y 20.3 LET)...

... debe recordarse que la jurisprudencia de este Tribunal ha insistido reiteradamente en la plena efectividad de los derechos fundamentales del trabajador en el marco de la relación laboral, ya que ésta no puede implicar en modo alguno la privación de tales derechos para quienes prestan servicio en las organizaciones productivas... En consecuencia, y como también ha afirmado este Tribunal, el ejercicio de tales derechos únicamente admite limitaciones o sacrificios en la medida en que se desenvuelve en el seno de una organización que refleja otros derechos reconocidos constitucionalmente en los arts. 38 y 33 CE y que impone, según los supuestos, la necesaria adaptabilidad para el ejercicio de todos ellos...

Debe por ello rechazarse la premisa de la que parte la Sentencia recurrida, consistente en afirmar que el centro de trabajo no constituye por definición un espacio en el que se ejerza el derecho a la intimidad por parte de los trabajadores, de tal manera que las conversaciones que mantengan los trabajadores entre sí y con los clientes en el desempeño de su actividad laboral no están amparadas por el art. 18.1 CE y no hay razón alguna para que la empresa no pueda conocer el contenido de aquéllas, ya que el referido derecho se ejercita en el ámbito de la esfera privada del trabajador, que en el centro de trabajo hay que entenderlo limitado a los lugares de descanso o esparcimiento, vestuarios, lavabos o análogos, pero no a aquéllos lugares en los que se desarrolla la actividad laboral...

...Tal afirmación resulta rechazable, pues no puede descartarse que también en aquellos lugares de la empresa en los que se desarrolla la actividad laboral puedan producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores, como podría serlo la grabación de conversaciones entre un trabajador y un cliente, o entre los propios trabajadores, en las que se aborden cuestiones ajenas a la relación

laboral que se integran en lo que hemos denominado propia esfera de desenvolvimiento del individuo (SSTC 231/1988, de 2 de diciembre, FJ 4 y 197/1991, de 17 de octubre, FJ 3, por todas). En suma, habrá que atender no solo al lugar del centro del trabajo en que se instalan por la empresa sistemas audiovisuales de control, sino también a otros elementos de juicio (si la instalación se hace o no indiscriminada y masivamente, si los sistemas son visibles o han sido instalados subrepticamente, la finalidad real perseguida con la instalación de tales sistemas, si existen razones de seguridad, por el tipo de actividad que se desarrolla en el centro de trabajo de que se trate, que justifique la implantación de tales medios de control, etc.) para dilucidar en cada caso concreto si esos medios de vigilancia y control respetan el derecho a la intimidad de los trabajadores. Ciertamente, la instalación de tales medios en lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos resulta, a fortiori, lesiva en todo caso del derecho a la intimidad de los trabajadores, sin más consideraciones, por razones obvias... Pero ello no significa que esa lesión no pueda producirse en aquellos lugares donde se realiza la actividad laboral, si concurre alguna de las circunstancias expuestas que permita calificar la actuación empresarial como ilegítima intrusión en el derecho a la intimidad de los trabajadores. Habrá, pues, que atender a las circunstancias concurrentes en el supuesto concreto para determinar si existe o no vulneración del art. 18.1 CE.

...su limitación [de los derechos fundamentales del trabajador] por parte de las facultades empresariales sólo puede derivar bien del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho (SSTC 99/1994, FJ 7, y 106/1996, FJ 4), bien de una acreditada necesidad o interés empresarial, sin que sea suficiente su mera invocación para sacrificar el derecho fundamental del trabajador (SSTC 99/1994, FJ 7, 6/1995, FJ 3 y 136/1996, FJ 7)...

Estas limitaciones o modulaciones tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes. Se trata, en definitiva, de la aplicación del principio de proporcionalidad...

La cuestión a resolver es, pues, si la instalación de micrófonos que permiten grabar las conversaciones de trabajadores y clientes en determinadas zonas... se ajusta en el supuesto que nos ocupa a las exigencias indispensables del respeto del derecho a la intimidad. Al respecto hemos de comenzar señalando que resulta indiscutible que la instalación de aparatos de captación y grabación del sonido en dos zonas concretas... no carece de utilidad para la organización empresarial, sobre todo si se tiene en cuenta que se trata de dos zonas en las que se producen transacciones económicas de cierta importancia. Ahora bien, la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación, habida cuenta de que la empresa ya disponía de otros sistemas de seguridad que el sistema de audición pretende complementar...

En resumen, la implantación del sistema de audición y grabación no ha sido en este caso conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial, pues la finalidad que se persigue (dar un plus de seguridad, especialmente ante eventuales reclamaciones de los clientes) resulta desproporcionada para el sacrificio que implica del derecho a la intimidad de los trabajadores (e incluso de los clientes...). Este sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores..., comentarios ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa. Se trata, en suma, de una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE, pues no existe argumento definitivo que

autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores... mantengan entre sí o con los clientes”.

Por otra parte, el tratamiento de datos personales está sometido al resto de los principios del tratamiento contenidos en el artículo 5 del RGPD. Destacaremos el principio de minimización de datos contenido en el artículo 5.1.c) del RGPD que dispone que los datos personales serán *“adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”*.

Esto significa que en un tratamiento concreto sólo pueden tratarse los datos personales oportunos, que vengan al caso y que sean los estrictamente necesarios para cumplir la finalidad para la que son tratados. El tratamiento debe ser ajustado y proporcional a la finalidad a la que se dirige. La pertinencia en el tratamiento de los datos debe producirse tanto en el momento de la recogida de los datos como en el posterior tratamiento que se realice de los mismos.

Conforme a lo antedicho, debe restringirse el tratamiento de los datos excesivos o bien procederse a la supresión de los mismos.

La aplicación del principio de minimización de datos al supuesto examinado comporta que el sistema de cámaras o videocámaras instalado no pueda obtener imágenes o sonidos afectando a la intimidad de los empleados, resultando desproporcionado captar imágenes o sonidos en espacios privados, tales como vestuarios, taquillas o zonas de descanso de trabajadores.

IV

Obligaciones en materia de videovigilancia

De conformidad con lo expuesto, el tratamiento de imágenes a través de un sistema de videovigilancia, para ser conforme con la normativa vigente, debe cumplir los requisitos siguientes:

1.- La personas físicas o jurídicas, públicas o privadas, pueden establecer un sistema de videovigilancia con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Se ha de valorar si la finalidad pretendida puede lograrse de otra forma menos intrusiva para los derechos y libertades de los ciudadanos. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios, considerando 39 del RGPD.

2.- Las imágenes obtenidas no puedan utilizarse para una finalidad ulterior incompatible con la que motivó la instalación del sistema de videovigilancia.

3.- Se deberá cumplir con el deber de informar a los afectados previsto en los artículos 12 y 13 del RGPD, y 22 de la LOPDGDD.

En tal sentido, el artículo 22 de la LOPDGDD prevé en relación con la videovigilancia un sistema de “información por capas”.

La primera capa ha de referirse, al menos, a la existencia del tratamiento (videovigilancia), la identidad del responsable, la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD y dónde obtener más información sobre el tratamiento de los datos personales.

Esta información se contendrá en un dispositivo colocado en un lugar suficientemente visible y debe suministrarse por adelantado.

La información de la segunda capa debe estar disponible en un lugar fácilmente accesible al afectado, ya sea una hoja informativa en una recepción, cajero, etc..., colocada en un espacio público visible o en una dirección web, y ha de referirse al resto de elementos del artículo 13 del RGPD.

4.- No pueden captarse imágenes de la vía pública, puesto que el tratamiento de imágenes en lugares públicos, salvo que concurra autorización gubernativa, sólo puede ser realizado por las Fuerzas y Cuerpos de Seguridad.

En algunas ocasiones, para la protección de espacios privados, donde se hayan instalado cámaras en fachadas o en el interior, puede ser necesario para garantizar la finalidad de seguridad la grabación de una porción de la vía pública.

Es decir, las cámaras y videocámaras instaladas con fines de seguridad no podrán obtener imágenes de la vía pública salvo que resulte imprescindible para dicho fin, o resulte imposible evitarlo por razón de la ubicación de aquéllas. Y, en tal caso extraordinario, las cámaras sólo podrán captar la porción mínima necesaria para preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Las cámaras instaladas no pueden obtener imágenes de espacio privativo de tercero y/o espacio público sin causa justificada debidamente acreditada, ni pueden afectar a la intimidad de transeúntes que transiten libremente por la zona.

No está permitida, por tanto, la colocación de cámaras hacia la propiedad privada de vecinos con la finalidad de intimidarlos o afectar a su ámbito privado sin causa justificada.

En ningún caso se admitirá el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular, no pudiendo afectar a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

No pueden captarse ni grabarse imágenes en espacios propiedad de terceros sin el consentimiento de sus titulares, o, en su caso, de las personas que en ellos se encuentren.

Resulta desproporcionado captar imágenes en espacios privados, tales como vestuarios, taquillas o zonas de descanso de trabajadores.

5.- Las imágenes podrán conservarse por un plazo máximo de un mes, salvo en aquellos supuestos en que se deban conservar para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

En este segundo supuesto, deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

6.- El responsable deberá llevar un registro de actividades de los tratamientos efectuados bajo su responsabilidad en el que se incluya la información a la que hace referencia el artículo 30.1 del RGPD.

7.- El responsable deberá realizar un análisis de riesgos o, en su caso, una evaluación de impacto en la protección de datos, para detectar los derivados de la implantación del sistema de videovigilancia, valorarlos y, en su caso, adoptar las medidas de seguridad apropiadas.

8.- Cuando se produzca una brecha de seguridad que afecte a los tratamientos de cámaras con fines de seguridad, siempre que exista riesgo para los derechos y libertades de las personas físicas, deberá notificarlo a la AEPD en un plazo máximo de 72 horas.

Se entiende por brecha de seguridad la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

9.- Cuando el sistema esté conectado a una central de alarma, únicamente podrá ser instalado por una empresa de seguridad privada que reúna los requisitos contemplados en el artículo 5 de la Ley 5/2014 de Seguridad Privada, de 4 de abril.

La Agencia Española de Protección de Datos ofrece a través de su página web [<https://www.aepd.es>] acceso a:

- . la legislación en materia de protección de datos personales, incluyendo el RGPD y la LOPDGDD (apartado “Informes y resoluciones” / “normativa”),
- . la Guía sobre el uso de videocámaras para seguridad y otras finalidades,
- . la Guía para el cumplimiento del deber de informar (ambas disponibles en el apartado “Guías y herramientas”).

También resulta de interés, en caso de realizar tratamientos de datos de bajo riesgo, la herramienta gratuita Facilita (en el apartado “Guías y herramientas”), que, mediante unas preguntas concretas, permite valorar la situación del responsable respecto del tratamiento de datos personales que lleva a cabo, y en su caso, generar diversos documentos, cláusulas informativas y contractuales, así como un anexo con medidas de seguridad orientativas consideradas mínimas.

V

Infracción administrativa

La reclamación se basa en la presunta ilicitud del sistema de videovigilancia instalado por la parte reclamada en el local donde desarrolla su actividad empresarial, en relación con la grabación de sonidos.

No resulta controvertido en este caso el hecho de que la parte reclamada es la titular y responsable del sistema de videovigilancia denunciado y, por tanto, la responsable de los tratamientos de datos que conlleva la utilización de dicho sistema. Y tampoco el hecho de que entre los tratamientos de datos realizados se contempla la recogida y almacenamiento de datos personales relativos a la voz de empleados y clientes.

Consta probado en las actuaciones, asimismo, que dicha instalación se realiza con fines de seguridad y control laboral.

Por ese motivo, con fecha 20/08/2018, la parte reclamada comunicó a los trabajadores afectados, entre los que figura la parte reclamante, la instalación del sistema de videovigilancia, con captación y grabación de imágenes y sonido, *“con la finalidad de dar cumplimiento al operativo de seguridad y para prevenir riesgos que afecten a la seguridad y protección de las personas, locales y bienes patrimoniales”* y para el *“control de la calidad y rendimiento laboral de los trabajadores así como verificación del cumplimiento... de sus obligaciones y deberes laborales”*.

La parte reclamada no aporta justificación suficiente sobre estos tratamientos de datos (grabación de sonidos). No tiene en cuenta la parte reclamada los límites previstos en el artículo 20.3 de la Ley del Estatuto de los Trabajadores (LET); lo establecido en el artículo 89.3 de la LOPDGDD, que admite la grabación de sonidos únicamente cuando resulten relevantes los riesgos y respetando los principios de proporcionalidad e intervención mínima; ni la doctrina del Tribunal Constitucional, ya expresada, según la cual la grabación de conversaciones entre trabajadores o entre éstos y clientes no se justifica por la verificación del cumplimiento por el trabajador de sus obligaciones o deberes.

El citado artículo 89 de la LOPDGDD, más allá de la prohibición de utilizar estos sistemas de videovigilancia y grabación de sonidos en *“lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos”*, expresamente y con carácter general, establece el sometimiento de tales sistemas al marco legal y con los límites inherentes al mismo, ya señalados anteriormente. Ello implica que no puede entenderse como legítimo, sin más condición, cualquier sistema que no incluya aquellos espacios.

En este caso, además, consta que uno de los micrófonos se instaló en el office utilizado por los trabajadores. Según ha quedado probado, el sistema incluyó la instalación de cuatro micrófonos *“ocultos”*: en el acceso al restaurante, en la sala donde están ubicadas las mesas y barra del establecimiento (más de 30 mesas de distintas dimensiones -entre y seis puestos- y 12 puestos de barra), en un office y en una estancia de pequeño tamaño cuyo uso no está especificado en el plano. Por tanto, resulta que alguno de estos dispositivos podría vulnerar la prohibición de instalar *“sistemas de grabación de sonidos... en lugares destinados al descanso o esparcimiento de los trabajadores..., tales como vestuarios, aseos, comedores y análogos”*, establecida en el citado artículo 89 de la LOPDGDD.

Por otra parte, en la información facilitada a los trabajadores se hace referencia a la *“facultada de vigilancia empresarial”*. Sobre esta cuestión, relativa a las posibilidades en cuanto a la adopción de medidas de vigilancia que atribuye al empresario su poder

de dirección, interesa destacar algunos de los aspectos declarados en la Sentencia del Tribunal Constitucional de fecha 10/04/2000, reseñada en el Fundamento de Derecho III:

“...esa facultad ha de producirse en todo caso, como es lógico, dentro del debido respeto a la dignidad del trabajador, como expresamente nos lo recuerda la normativa laboral (arts. 4.2.e y 20.3 LET)...”.

“Debe por ello rechazarse... que las conversaciones que mantengan los trabajadores entre sí y con los clientes en el desempeño de su actividad laboral no están amparadas por el art. 18.1...”.

“...su limitación [de los derechos fundamentales del trabajador] por parte de las facultades empresariales sólo puede derivar bien del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho (SSTC 99/1994, FJ 7, y 106/1996, FJ 4), bien de una acreditada necesidad o interés empresarial, sin que sea suficiente su mera invocación para sacrificar el derecho fundamental del trabajador (SSTC 99/1994, FJ 7, 6/1995, FJ 3 y 136/1996, FJ 7)...”.

Estas limitaciones o modulaciones tienen que ser las indispensables y estrictamente necesarias...”.

“...la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación, habida cuenta de que la empresa ya disponía de otros sistemas de seguridad que el sistema de audición pretende complementar...”.

Tampoco explica qué puede aportar la grabación de conversaciones entre los trabajadores, entre sí, entre los trabajadores y los clientes, o de éstos últimos entre sí, en orden a acreditar aquellas circunstancias, que no aporte la sola grabación de imágenes.

Asimismo, interesa destacar nuevamente que la grabación de sonidos incluye la voz de clientes de la parte reclamada (dos dispositivos instalados en la zona de clientes, en el acceso al restaurante y en la sala donde están ubicadas las mesas y barra del establecimiento), los cuales no tienen conocimiento de la existencia de los micrófonos.

En consecuencia, en este caso, se entiende desproporcionada la captación de la voz tanto de los trabajadores como de clientes de la parte reclamada para la función de videovigilancia pretendida, para el control del cumplimiento por los trabajadores de sus obligaciones y deberes laborales. Se tiene en cuenta que la grabación de voz supone una mayor intromisión en la intimidad.

Se considera que la parte reclamada realizó tratamientos de datos sin disponer de base legítima, vulnerando lo establecido en el artículo 6 del RGPD, por lo que podrían suponer la comisión de una infracción tipificada en el artículo 83.5 del RGPD, que dispone lo siguiente:

“Las infracciones de las disposiciones siguientes se sancionarán, 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;”.

A efectos del plazo de prescripción de las infracciones, la infracción señalada en el párrafo anterior se considera muy grave conforme al artículo 72.1.b) de la LOPDGDD, que establece que:

“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 Sanción

El artículo 58.2 del RGPD establece:

“Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(...)

d) ordenar al responsable o encargado de 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;

(...)

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular”.

Según lo dispuesto en el artículo 83.2 del RGPD, la medida prevista en el artículo 58.2.d) del citado Reglamento es compatible con la sanción consistente en multa administrativa.

Con respecto a las infracciones del artículo 6 del RGPD, atendiendo a los hechos expuestos, se considera que la sanción que correspondería imponer es de multa administrativa.

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.

A fin de determinar la multa administrativa a imponer se han de observar las previsiones del artículo 83.2 del RGPD y del artículo 76 de la LOPDGDD, respecto al apartado k) del citado artículo 83.2 RGPD.

En este caso, se consideran las siguientes circunstancias como agravantes:

. Artículo 83.2.a) del RGPD: *“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”.

. La duración de la infracción, considerando que la instalación de los dispositivos de captación y grabación de voz tuvo lugar en agosto de 2018.

. El número de interesados: la presunta infracción afecta a todos los trabajadores y clientes de la parte reclamada.

Por otra parte, se estima que concurren como atenuantes las circunstancias siguientes:

. Artículo 76.2.b) de la LOPDGDD: *“b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales”.*

La escasa vinculación de la parte reclamada con la realización de tratamientos de datos personales, considerando la actividad que desarrolla.

. Artículo 83.2.k) del RGPD: *“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”.*

La condición de pequeña empresa de la parte reclamada y su volumen de negocio. (...).

Considerando los factores expuestos, la valoración que alcanza la multa por la infracción del artículo 6 del RGPD es de 20.000 euros (veinte mil euros).

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER A MUXERS CONCEPT, S.L., con NIF B87345369, por una infracción del Artículo 6 del RGPD, tipificada en el Artículo 83.5.a) del RGPD, una multa de 20.000 euros (veinte mil euros).

SEGUNDO: NOTIFICAR la presente resolución a MUXERS CONCEPT, S.L.

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **ES00 0000 0000 0000 0000 0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago

voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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.

Finalmente, se señala que conforme a lo previsto en el art. 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://sedeagpd.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.

938-050522

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