936-031219

- **Procedimiento Nº: PS/00473/2019**

RESOLUCIÓN R/00258/2020 DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

En el procedimiento sancionador PS/00473/2019, instruido por la Agencia Española de Protección de Datos a ***HAPPY FRIDAY, S.L.***, vista la denuncia presentada por ***A.A.A.***, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 2 de abril de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***HAPPY FRIDAY, S.L.*** (en adelante, el reclamado), mediante el Acuerdo que se transcribe:

<<

Procedimiento Nº: PS/00473/2019

935-240719

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad, HAPPY FRIDAY, S.L., con CIF: B54660980, titular de la página web *https://happyfridayhome.com*, (en adelante, "la entidad reclamada"), en virtud de denuncia presentada por ***D. A.A.A.***, (en adelante, "el reclamante") y teniendo como base los siguientes:

HECHOS

PRIMERO: Con fecha 10/05/19, tiene entrada en esta Agencia, denuncia presentada por el reclamante en la que indica, entre otras, lo siguiente:

"En la empresa Happy Friday, SL, se está realizando mal todo, respecto al tratamiento de datos de carácter personal y otros: -Se trabaja con carpetas personales compartidas en el servidor donde se almacenan todos los ficheros que cada uno guarda de su trabajo diario en su propia carpeta personal. Carpetas accesibles por cualquier otro usuario indistintamente del departamento al que corresponda, sin ningún tipo de autentificación de servidor, sin requerimiento de ninguna contraseña o tipo de permisos. Cualquiera puede acceder a cualquier documento de otro trabajador indistintamente de su perfil, departamento o la sensibilidad de la información de la que se trate.

No se requiere credenciales para el inicio de sesión, ni contraseña para bloqueo de pantalla, etc. Además, todos los equipos utilizan software ilegal tanto a nivel de sistema operativo como de aplicaciones, con el riesgo que ello Supone. Y sin la seguridad de las actualizaciones que suelen proporcionar los fabricantes de software. Tratando miles de datos de clientes accesibles para cualquiera de los 25 trabajadores sin ningún tipo de control. Pues en la aplicación de gestión (Eneboo) se pide inicio de

sesión, pero todo el mundo puede acceder a cualquier parte de la aplicación indistintamente de su rol y departamento sin ningún tipo de autentificación ni log de quien ha realizado cada acción. También considero que no están actuando conforma a la legalidad vigente en lo que al tratamiento de datos de uso personal se refiere:

Al entrar en la web https://happvfridavhome.com se abre un pop-up solicitando la suscripción al boletín con un "Acepto los Términos y Condiciones", pero no se advierte ni informa de las cookies que utilizan y del rastreo que realizan desde que se accede a la web. Tampoco se pide ningún consentimiento para la recopilación de esta información. Cookies que se ponen ya en marcha en la portada sin aceptarlas, ni habernos mostrado la información de las mismas. Como pueden ver no indican nada en la siguiente página https://happvfridavhome.com/es/cookies Se puede navegar con la total funcionalidad en la web sin haber aceptado ninguna política de cookies, privacidad".

SEGUNDO: A la vista de los hechos expuestos en la reclamación y de los documentos aportados por el reclamante, la Subdirección General de Inspección de Datos procedió a realizar actuaciones para su esclarecimiento, al amparo de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD). Así, con fecha 12/07/19, se dirige un requerimiento informativo a la entidad reclamada.

TERCERO: Con fecha 08/08/19, la entidad reclamada envía a esta Agencia escrito en el que, entre otras, informa de los siguiente:

"Sobre las medidas y normas relativas a la identificación y autentificación del personal autorizado a acceder a los datos personales.

a).- Todos los usuarios del sistema tienen asignado un identificador y una contraseña. El sistema de autenticación se basa en un entorno de clave de acceso bajo un sistema operativo Microsoft Windows 10. El usuario introduce su identificador (que le identifica como usuario autorizado al acceso) y su contraseña (que le autentifica como el usuario identificado), que son verificados en el propio ordenador, el cual le reconoce como usuario del sistema, permitiéndole acceder a los directorios, archivos y bases de datos para el desempeño de su trabajo.

b).- Las contraseñas constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

- *El archivo de las contraseñas deberá estar protegido (en soporte informático serían inteligibles mediante el propio sistema de encriptación que utiliza el sistema operativo) y bajo la responsabilidad del administrador del sistema.*
- *Las contraseñas serán de 13 caracteres alfanuméricos, modificándose por el responsable del fichero cada 12 meses.*
- *El Responsable del Fichero, o por cuenta de éste el Administrador del Sistema encargado del tratamiento, eliminará las contraseñas de los usuarios que se hayan dado de baja en la organización.*

c).- El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos distintos de los autorizados de la siguiente forma:

- *Se confeccionarán los distintos perfiles de usuario en los que se autorizarán / denegarán los diferentes accesos a las funciones permitidas.*
- *Se informará al personal de las aplicaciones, herramientas y documentación a la que tiene acceso para realizar sus funciones.*
- *Solo el responsable del fichero, está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.*

d).- En el Anexo II, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará cuando sea necesario por modificaciones en el personal, por parte del responsable del fichero.

- *De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.*
- *Los documentos manuales se encuentran en armarios cerrados en cada puesto de trabajo de los usuarios autorizados.*

e).- Sobre los criterios de archivo y almacenamiento de la información en ficheros manuales o no automatizados.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios establecidos por el responsable del fichero: En la oficina se dispone de un área de trabajo compuesta de escritorios con ordenadores y unos archivadores metálicos con llave, en los que se guarda la documentación manual, correctamente identificadas su contenido y al acceso únicamente del personal autorizado para ello.

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos mencionados anteriormente, por estar trabajando con ellos, las personas que se encuentren al cargo de los mismos deberán custodiarlos e impedir en todo momento que pueda ser accedida por personas no autorizadas.

La oficina está situada en una nave industrial. Para acceder a ella se debe llamar a un timbre exterior, entrar previa autorización, atravesar la nave y al fondo, subiendo unas escaleras, se accede a la segunda planta de la nave, donde está ubicada la gestión administrativa de la empresa.

La seguridad de los datos personales de los Ficheros no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos. Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero.

- *El responsable del Fichero será responsable de obtener periódicamente una copia de seguridad, a efectos de respaldo y recuperación en caso de fallo.*
- *Se realiza una copia de seguridad diariamente en el Dispositivo de almacenamiento (NAS) ubicado en la empresa, así como otra copia paralela en otro Dispositivo de almacenamiento (NAS) ubicado en una Nave utilizada como almacén, dentro de un armario cerrado con llave donde sólo tiene acceso el Responsable del Fichero y persona autorizado.*

Con este método actual que tenemos la empresa garantiza un nivel de seguridad adecuado en el tratamiento de datos personales.

f).- Sobre las Cookies.

Referente a las medidas adoptadas para facilitar información clara y completa sobre la utilización de Cookies, los fines del tratamiento de los datos recabados por éstas, y el procedimiento para obtener el consentimiento de los usuarios acerca de su instalación en el navegador, les informamos que desde la puesta en funcionamiento de nuestra WEB sí que existe un aviso a los usuarios en la parte inferior de la página, apareciendo un letrero de información y autorización para el uso de Cookies enmarcado en fondo negro sobre letras blancas que podían aceptar u obtener más información, cumpliendo así con nuestra obligación.

Después de haber recibido esta notificación y tras una reunión de Dirección con el Departamento Informático hemos visto conveniente mejorar nuestra web haciendo más visible el apartado relativo a las Cookies, para así tener una mayor transparencia para los usuarios que utilizan nuestra Web. Pueden revisarlo en: https://happyfridayhome.-com/ ".

CUARTO: Con fecha 09/10/19, A la vista de los hechos expuestos en la información aportada por la entidad reclamada, la Subdirección General de Inspección de Datos procedió a requerirla información adicional sobre, Políticas de seguridad o en su defecto los siguientes procedimientos: Procedimiento de autenticación de usuarios; Procedimiento de Control de Acceso; Relación de usuarios con acceso a casa sistema de información (Anexo II) y Procedimiento de almacenamiento y copias de seguridad.

QUINTO: Con fecha 10/10/19, la entidad reclamada remite a esta Agencia, escrito en el que, entre otras, informa de lo siguiente:

a).- Todos los usuarios tienen asignado un identificador y una contraseña. El sistema de autenticación se basa en el sistema operativo Microsoft Windows 10.

El usuario introduce su identificador (que le identifica como usuario autorizado) y su contraseña (que le autentifica como el usuario), que son verificados en el propio ordenador, el cual le reconoce como usuario, permitiéndole acceder a los directorios, archivos y bases de datos para el desempeño de su trabajo. Las contraseñas son de 12 caracteres alfanuméricos, modificándose por el responsable del fichero cada 12 meses.

El personal sólo accede a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del Fichero establece mecanismos para evitar que un usuario pueda acceder a recursos distintos de los autorizados de la siguiente forma:

- *Se han confeccionado los distintos perfiles de usuario en los que se autorizarán / denegarán los diferentes accesos a las funciones permitidas.*
- *Se ha informado al personal de las aplicaciones, herramientas y documentación a la que tiene acceso para realizar sus funciones.*

Exclusivamente el responsable del fichero está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos. Los documentos manuales se encuentran en 2 armarios cerrados con llave, y solo acceden los usuarios autorizados.

b).- Almacenamiento de la información en ficheros manuales o no automatizados:

En la oficina se dispone de un área de trabajo compuesta de escritorios con ordenadores y unos archivadores metálicos con llave, en los que se guarda la documentación manual, correctamente identificadas su contenido y al acceso únicamente del personal autorizado para ello.

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos mencionados anteriormente, por estar trabajando con ellos, las personas que se encuentren al cargo de los mismos deberán custodiarlos e impedir en todo momento que pueda ser accedida por personas no autorizadas.

La oficina está situada en una nave industrial. Para acceder a ella se debe llamar a un timbre exterior, entrar previa autorización, atravesar la nave y al fondo, subiendo unas escaleras, se accede a la segunda planta de la nave, donde está ubicada la gestión administrativa de la empresa.

c).- Almacenamiento de la información en ficheros informáticos.

Todos los archivos se encuentran ubicados en el servidor de la empresa (SERVER 2019). Los usuarios tienen asignado un identificador y una contraseña. El acceso es mediante el PC de cada usuario en entorno Windows 10 con nombre de usuario y contraseña y tienen acceso únicamente a los archivos que usan y para los que están debidamente autorizados.

d).- Copias de Seguridad:

El responsable del Fichero es responsable de obtener periódicamente una copia de seguridad del fichero.

Se realiza una copia de seguridad diariamente en el Dispositivo de almacenamiento (NAS), ubicado en la empresa, así como otra copia paralela en otro Dispositivo de almacenamiento (NAS) ubicado en una Nave utilizada como almacén, dentro de un armario cerrado con llave donde sólo tiene acceso el Responsable del Fichero y personal autorizado.

SEXTO: A la vista de los hechos denunciados, de conformidad con las evidencias de que se dispone, la Inspección de Datos de esta Agencia Española de Protección de Datos considera que la política de cookies que se realiza por la entidad reclamada, no

cumple las condiciones que impone la normativa vigente, por lo que procede la apertura del presente procedimiento sancionador.

FUNDAMENTOS DE DERECHO

I
Competencia

- Sobre las medidas de seguridad:

En virtud de los poderes que el art 58.2 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/16, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (RGPD) reconoce a cada Autoridad de Control y, según lo establecido en los arts. 47, 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 (LOPDGDD), la Directora de la Agencia Española de Protección de Datos es competente para iniciar este procedimiento.

Los apartados 1) y 2), del artículo 58 el RGPD, enumeran, respectivamente, los poderes de investigación y correctivos que la autoridad de control puede disponer al efecto, mencionando en el punto 1.d), el de: “notificar al responsable o encargo del tratamiento las presuntas infracciones del presente Reglamento” y en el 2.i), el de: “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.”.

- Sobre la Política de Cookies:

De conformidad con lo establecido en el art. 43.1, párrafo segundo, de la de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI), es competente para iniciar y resolver este Procedimiento Sancionador, la Directora de la Agencia Española de Protección de Datos.

II

A).- Sobre las medidas de seguridad en los sistemas informáticos:

En el presente caso, el reclamante denuncia la inexistencia de medidas de seguridad, en la gestión del sistema informático existente en la empresa reclamada.

No obstante, de la información y documentación aportada por la empresa, se desprenden varios aspectos que deben tenerse en cuenta:

a).- Se dispone de un área de trabajo compuesta de escritorios con ordenadores y unos
archivadores metálicos con llave, en los que se guarda la documentación manual, correctamente identificados.

b).- El acceso únicamente se permite al personal autorizado para ello. En tanto los documentos con datos personales no se encuentren archivados en los dispositivos

mencionados anteriormente, por estar trabajando con ellos, las personas que se encuentren al cargo de los mismos son los responsables de custodiarlos e impedir que pueda ser utilizados por otras personas no autorizadas.

c).- La oficina está situada en una nave industrial. Para acceder a ella se debe llamar a un timbre exterior, entrar con autorización, atravesar la nave y acceder a la segunda planta donde está ubicada el área de gestión administrativa de la empresa.

d).- Sobre el almacenamiento de la información en ficheros informáticos: todos los archivos se encuentran ubicados en el servidor de la empresa (SERVER 2019). Los usuarios tienen asignado un identificador y una contraseña. El acceso es mediante el PC de cada usuario en entorno Windows 10, con usuario y contraseña. Solo se tiene acceso a los archivos que se usan y para los que están debidamente autorizados.

e).- Sobre las copias de seguridad: el responsable del fichero es el encargado de obtener periódicamente una copia de seguridad del fichero. Se realiza una copia de seguridad diariamente en el dispositivo de almacenamiento (NAS), ubicado en la empresa, así como otra copia paralela en otro dispositivo de almacenamiento (NAS), ubicado en otra nave, dentro de un armario cerrado con llave donde sólo tiene acceso el responsable del fichero y el personal autorizado.

f).- Según el responsable, la compañía ha realizado la adaptación al nuevo Reglamento en el cual se incluye un Documento de Seguridad sobre Medidas, Normas, Procedimientos, Reglas y Estándares de Seguridad, en el cual se explicitan las medidas y normas relativas a la identificación y autenticación del personal con acceso a los datos personales basado en un entorno de clave de acceso bajo sistema Windows 10.

g).- Respecto al Control de Acceso manifiesta que el personal sólo accede a aquellos datos y recursos que precise para el desarrollo de sus funciones para lo cual el responsable establecerá mecanismos para evitar que un usuario acceda a recursos para los que no tiene privilegios en base a la confección de distintos perfiles de usuario en los que se autorizarán/denegarán los accesos a las funciones permitidas. Habla de que se informará al personal de las aplicaciones, herramientas y documentación a las que tiene acceso para realizar sus funciones. El Anexo II, enviado a esa Agencia, incluye una relación de usuarios actualizada, con el acceso permitido a cada sistema de información, así como el tipo de acceso.

En lo que respecta a la seguridad de los sistemas informáticos de la entidad, indicar que, el RGPD instaura un nuevo sistema de protección de datos basado en la responsabilidad proactiva. Esto quiere decir que, deben ser los responsables del tratamiento los que establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo.

Por ello, de la información y documentación aportada por la entidad reclamada no se desprende que la política de seguridad, implantada en sus sistemas informáticos, contravengan las directrices marcadas por el RGPD a este respecto.

III

B).- Sobre la Política de Cookies, y siguiendo las recomendaciones de la "Guía sobre Cookies" publicada por la Agencia Española de Protección de datos, en noviembre de 2019, al entrar en la página web *https://happvfridavhome.com*, se comprueba las siguientes características:

a) En la página inicial (primera capa), existe un banner con la siguiente leyenda:

"Utilizamos cookies propias y de terceros para mejorar nuestros servicios y mostrarte publicidad relacionada con tus preferencias, mediante el análisis de tus hábitos de navegación. Puedes obtener más información, o bien conocer cómo cambiar la configuración, en nuestra Política de Cookies. Pulsa ACEPTAR para confirmar que has leído y aceptado la información presentada. Después de aceptar, no volveremos a mostrarte este mensaje"

a) En la segunda capa, "Política de Cookies". Si se accede a la "Política de Cookies", se proporciona información sobre algunos aspectos de las cookies, como por ejemplo, qué son, los tipos de cookies que existen pero no se da información de las cookies, tanto propias y de terceros, que se cargan cuando se navega por la web ni del tiempo que permanecerán instaladas en el equipo terminal. Tampoco se posibilita, en esta segunda capa, un mecanismo que permita gestionar la instalación de cookies de forma granular y/o de rechazar todas las cookies.

IV

Así las cosas, en el banner sobre cookies de la primera capa, la información sobre las cookies facilitada no permitir a los usuarios entender sus finalidades y el uso que se les dará ya que se utiliza un lenguaje poco claro, con frases como "*(…) mejorar nuestros servicios (…)"* sin que se dé más información al respecto.

En la segunda capa, a la cual se accede a través del link, "Política de Cookies", no se informa del tipo de cookies que utiliza, si son propias o de terceros ni el periodo de conservación de las mismas en el ordenador; no se informa de si existe o no trasferencia internacional de datos o si existe elaboración de perfiles. Tampoco se incluye un panel para gestionar cookies de forma granular ni otro que permita, en su caso, rechazar todas las cookies. La página solo se limita a ofrecer información sobre herramientas que permiten deshabilitar cookies y remite a la configuración del navegador para ello.

Los hechos expuestos podrían suponer por parte de la entidad reclamada la comisión de la infracción del artículo 22.2 de la LSSI, según el cual: *"Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con*

arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario".

Esta Infracción estas tipificada como leve en el artículo 38.4 g), de la citada Ley, que considera como tal: "Utilizar dispositivos de almacenamiento y recuperación de datos cuando no se hubiera facilitado la información u obtenido el consentimiento del destinatario del servicio en los términos exigidos por el artículo 22.2.", pudiendo ser sancionada con multa de hasta 30.000 €, de acuerdo con el artículo 39 de la citada LSSI.

V

Tras las evidencias obtenidas en la fase de investigaciones previas, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el art. 40 de la LSSI:

- La existencia de intencionalidad, expresión que ha de interpretarse como equivalente a grado de culpabilidad de acuerdo con la Sentencia de la Audiencia Nacional de 12/11/07 recaída en el Recurso núm. 351/2006, correspondiendo a la entidad denunciada la determinación de un sistema de obtención del consentimiento informado que se adecue al mandato de la LSSI.

- Plazo de tiempo durante el que ha venido cometiendo la infracción, al ser la reclamación mayo de 2019, (apartado b).

Con arreglo a dichos criterios, se estima adecuado imponer a la entidad reclamada una sanción de 2.500 euros (dos mil quinientos euros), por la infracción del artículo 22.2 de la LSSI. Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

INICIAR: PROCEDIMIENTO SANCIONADOR a la entidad HAPPY FRIDAY, S.L., con CIF: B54660980, titular de la página web *https://happvfridavhome.com* , por Infracción del artículo 22.2) de la LSSI, sancionable conforme a lo dispuesto en los art. 39.1.c) y 40) de la citada Ley, respecto de su Política de Cookies.

NOMBRAR: como Instructor a ***D. R.R.R.,*** y Secretaria, en su caso, a ***Dª S.S.S.***, indicando que cualquiera de ellos podrá ser recusado, en su caso, conforme a lo establecido en los art 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

INCORPORAR: al expediente sancionador, a efectos probatorios, la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados

por la Subdirección General de Inspección de Datos durante la fase de investigaciones, todos ellos parte del presente expediente administrativo.

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 una multa de 2.500 euros por la infracción del artículo 22.2 de la LSSI, sin perjuicio de lo que resulte de la instrucción.

REQUERIR: a la entidad HAPPY FRIDAY, S.L., para que tome las medidas adecuadas para incluir en las páginas web de su titularidad, información sobre las cookies que se instalan y un mecanismo que permita habilitar o rechazar todas las cookies y otro que permita habilitar las cookies de forma granular para poder administrar las preferencias del usuario.

NOTIFICAR: el presente acuerdo de inicio de expediente sancionador a la entidad HAPPY FRIDAY, S.L., otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes.

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).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, en caso de que la sanción a imponer fuese de multa, 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, equivalente en este caso a 500 euros. Con la aplicación de esta reducción, la sanción quedaría establecida en 2000 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 una reducción de un 20% del importe de la misma, equivalente en este caso a 500 euros. Con la aplicación de esta reducción, la sanción quedaría establecida en 2000 euros y su pago implicará la terminación del procedimiento.

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 1.500 euros (mil quinientos 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.

Si se optara por proceder al pago voluntario de cualquiera de las cantidades señaladas

anteriormente, deberá hacerlo efectivo mediante su ingreso en la cuenta ***nº ES00 0000 0000 0000 0000 0000*** abierta a nombre de la Agencia Española de Protección de Datos en el Banco 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.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de 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. 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.

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

>>

SEGUNDO**:** En fecha 15 de junio de 2020, el reclamado ha procedido al pago de la sanción en la cuantía de **1500 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.
TERCERO**:** El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en el art. 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), la Directora de la Agencia Española de Protección de Datos es competente para sancionar las infracciones que se cometan contra dicho Reglamento; las infracciones del artículo 48 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en lo sucesivo LGT), de conformidad con lo dispuesto en el artículo 84.3 de la LGT, y las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en lo sucesivo LSSI), según dispone el artículo 43.1 de dicha Ley.

II

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.*

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **PS/00473/2019**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***HAPPY FRIDAY, S.L.***.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.
Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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.

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