- **Expediente N.º: EXP202304685**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 5 de julio de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202304685 (PS/00238/2024)

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: ***A.A.A. y B.B.B.*** (en adelante, la parte reclamante) con fecha 31 de marzo de 2023 interpuso reclamación ante la Agencia Española de Protección de Datos. Los hechos reclamados ponen de manifiesto una posible infracción imputable a **UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA** con NIF **W8266168G** (en adelante, UNIQLO).

Los hechos conocidos son los siguientes:

La primera reclamación interpuesta por la parte reclamante, que prestaba servicios en la entidad reclamada, manifiesta que con fecha 8 de agosto de 2022, tras solicitar su nómina a la entidad, recibió un correo electrónico con un documento PDF adjunto que incluía su nómina y la de 446 trabajadores más de la plantilla.

Junto con la reclamación aporta el documento PDF que contiene las nóminas de 447 trabajadores de la entidad reclamada, constando nombre y apellidos, DNI, número de afiliación de la SS y número de cuenta bancaria, entre otros datos.

La segunda reclamación se origina a partir de recibir la comunicación informativa de la brecha, enviada por UNIQLO a los empleados afectados mediante correo electrónico. La parte reclamante de esta segunda reclamación, que manifiesta pertenecer al Comité de Empresa, aporta captura de pantalla del correo recibido el 4 de mayo de 2023.

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 dicha reclamación a UNIQLO, 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.

UNIQLO responde al traslado de la reclamación con fecha 18 de mayo de 2023. Sin embargo, se observa que, de la respuesta al traslado de la reclamación, se infiere una posible vulneración de la normativa de protección de datos.

TERCERO: Con fecha 8 de junio de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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 VIII, de la LOPDGDD.

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

1.- Constatación de los hechos reclamados.

Como primer aspecto de estas actuaciones de investigación se ha analizado la información proporcionada en la reclamación y por la parte reclamada, tanto en el traslado como en posteriores requerimientos en relación con el origen del incidente.

El objeto causante de la brecha sería un archivo PDF que contendría la información de toda la plantilla de UNIQLO relativa a las nóminas del mes de julio. Dicho archivo ha sido aportado por la parte reclamante y se ha procedido a contrastar la información contenida en él, así como la causa de que fuera enviado indebidamente a una persona no autorizada.

La parte reclamada admite los hechos reclamados: Con motivo de la terminación del contrato laboral de la parte reclamante, esta solicitó su nómina de julio de 2022 al departamento de recursos humanos. Manifiestan que, en el contexto del intercambio de información por correo electrónico, su departamento de recursos humanos envió por error el archivo indicado, con la información de toda la plantilla. Atribuyen este hecho a un error humano, tanto en el documento de notificación de brecha de datos personales: "*the breach was caused by an HR staff by mistake (human error) who did*

not follow the internal process" (en castellano: "*la brecha fue causada por un error del personal de RRHH (error humano) que no siguió el proceso interno*") y en numerosos puntos de las alegaciones "*el Empleado de RRHH remitió un archivo que, por error, contenía las nóminas del mes de julio de todos los trabajadores de Uniqlo y los siguientes datos personales:..*".

La parte reclamada manifiesta que el archivo contenía la información 446 trabajadores de UNIQLO. Tras la revisión del listado proporcionado en la reclamación, se constata que, aunque el archivo contiene 471 nóminas, corresponden a 447 empleados, ya que hay algunos casos en que una misma persona tenía asociada distintas nóminas durante el mes por diferentes motivos laborales (cambio de contrato, bajas, etc.). En la reclamación se indica la cifra de 470 trabajadores, sin contar al propio empleado reclamante, pero la cifra correcta sería efectivamente de 446.

La parte reclamada manifiesta que dicho archivo contenía los siguientes datos personales: nombre, apellido, número de DNI/NIE, número de la Seguridad Social, número de cuenta bancaria y retribución percibida. Se comprueba que las manifestaciones de la parte reclamada son acordes a la información proporcionada por la parte reclamante y el archivo filtrado aportado.

Adicionalmente, la parte reclamada aporta comunicaciones mantenidas en ese momento entre la parte reclamante y la persona que intervino de recursos humanos, a través de correo electrónico. Mediante estos mensajes se puede acreditar la fecha del incidente, enviándose el archivo el 8 de agosto de 2022. Se desprende por las comunicaciones intercambiadas a partir de ello que la parte reclamante eliminaría el archivo ("*Para tu tranquilidad, te informo de que no llegué a descargarlo, lo abrí online y en cuanto vi la primera página lo cerré, así que no te preocupes que no está en mis archivos*"), hecho que pudo condicionar la actuación del personal de la parte reclamada.

Según manifiesta la parte reclamada, el empleado de recursos humanos que remitió el archivo no informó de ellos a sus responsables ni lo puso en conocimiento de la empresa, por lo que la brecha no trascendió ni se actuó de forma proactiva ante ella. Únicamente se tuvo constancia, tal como manifiestan, cuando recibieron la notificación del traslado de la reclamación: "*el pasado 18 de abril de 2023 Uniqlo recibió una notificación de la AEPD por la que se le daba traslado de la reclamación presentada y se le requería cierta información. Fue en este preciso instante en el que Uniqlo, como organización empresarial, pudo conocer el incidente de seguridad del pasado agosto, hasta entonces, desconocido*".

2.- Comunicación informativa de la brecha.

2.1. Notificación a la autoridad de control.

Puesto que la información de esta brecha a la Agencia llegó a través de reclamación, se solicitó a la parte reclamada la motivación de por qué no fue notificada la brecha.

Como se ha indicado en el punto anterior, la argumentación presentada por la parte reclamada es que directamente desconocían la existencia de la brecha hasta que recibieron el traslado de la reclamación. Internamente culpan de esta situación a la persona de recursos humanos que incurrió en el envío de la información: "*el empleado*

de RRHH – en un flagrante incumplimiento de las políticas internas de Uniqlo – no informó en ningún momento a su superior jerárquico ni a la dirección de Uniqlo del incidente, motivo por el que la compañía no pudo conocer en tiempo y forma que éste se había producido y, por consiguiente, tampoco pudo noticiar a la AEPD de conformidad con el artículo 33 del Reglamento 2016/769 General de Protección de Datos"

Posteriormente realizaron la notificación formal de la brecha de datos personales, a fecha 24 de abril de 2023, y se incorporó al expediente. En dicha notificación constan los siguientes puntos relevantes:

- Responsable: UNIQLO EUROPE LTD, sucursal en España.
- Encargado: No hay encargado del tratamiento.
- Afectados: 471 empleados.
- Datos afectados: Datos básicos de contacto, número de identidad, datos económicos (sin datos de pago) y datos de contacto.
- Causa de la brecha: Accidental, de origen interno. Se aporta la explicación previamente mencionada en el punto 1 del informe relativa al error de recursos humanos.
- Consecuencias para los afectados: Afectada la confidencialidad. Podrían sufrir inconvenientes severos como phishing o intentos de suplantación, aunque se considera improbable que se materialice.
- Transfronteriza: No, únicamente en España.
- Menores: No hay menores entre los afectados.

2.2. Comunicación a los interesados:

Por otra parte, se requirió la información relativa a la comunicación a los interesados. La parte reclamada manifiesta que se realizó la comunicación informándoles del incidente a los pocos días de que tuvieron constancia del mismo, el 4 de mayo de 2023.

Aportan la comunicación remitida, que dispone de versión en castellano y en inglés. En ella se informa del incidente, explicando las causas y su magnitud con un lenguaje claro y conciso ("*el marco de la respuesta a una solicitud legítima, un archivo con su nómina correspondiente al mes de julio de 2022 fue enviado por error a una antigua persona trabajadora por parte de UNIQLO. La información que contiene una hoja de nómina incluye los siguientes datos personales: nombre, dirección, número de DNI/NIE, número de la Seguridad Social, número de la cuenta bancaria, salario y su desglose*"). Se reitera que no se tuvo constancia a nivel de dirección hasta que se comunicó por la AEPD, justificando así el decalaje de varios meses entre los hechos y la comunicación. Se facilita un correo electrónico de contacto para consultas

adicionales. Manifiestan haber recibido 10 comunicaciones al respecto, que habrían sido debidamente atendidas.

En la comunicación se manifiesta que no se tiene constancia de evidencias de exfiltración de los datos personales y se indica una referencia al INCIBE (Instituto Nacional de Ciberseguridad) para que los afectados puedan consultar recursos adicionales de ciberseguridad. No se concretan las posibles consecuencias que podría tener esta brecha, aunque se manifiesta: "*recomendamos que esté atento a cualquier riesgo potencial que pudiera derivarse de un uso indebido de sus datos personales*".

Por último, se indican las medidas que tomará UNIQLO para tratar de garantizar que no se produzcan más incidentes de este tipo: formación para el personal en ciberseguridad y privacidad de los datos, junto con la revisión de los procedimientos y políticas internas.

Adicionalmente al texto de la comunicación se aporta un cuadro de 15 preguntas y respuestas remitido a los afectados, que sintetizan la descripción de la brecha y los puntos comentados anteriormente. También se aporta un correo dirigido al Comité de Empresa, en la misma fecha, informando de este suceso y solicitando su colaboración.

Manifiestan que realizaron la comunicación por correo electrónico a la totalidad de los afectados, compuesta por 287 empleados y 160 exempleados en mayo de 2023, al no tener ya relación laboral con un importante grupo de los afectados. Teniendo en cuenta que entre los trabajadores también se encontraba la primera persona reclamante, la comunicación se habría realizado a la totalidad de los afectados. Se ha requerido acreditación de que la comunicación se ha realizado de forma efectiva a todo el personal afectado, pero no se ha recibido confirmación al respecto, aunque sí se aportan muestras de los correos dirigidos tanto a trabajadores en activo como a exempleados.

El contenido de la comunicación se aporta por doble partida, ya que la segunda reclamación también lo adjunta. En dicha reclamación, que proviene de una persona que manifiesta ser del Comité de Empresa, se indica "*la empresa está dirigiendo un correo electrónico (se adjunta) a todas las personas trabajadoras en el cual comunica y reconoce que ha existido una comunicación a terceras personas la cual contenía datos de carácter personal*", por lo que puede confirmarse que la comunicación se ha realizado de manera efectiva a, al menos, todo el personal en activo en esos momentos.

3.- Gestión de las nóminas.
Puesto que la brecha se ha ocasionado con motivo de la gestión de nóminas de la empresa, se ha profundizado en su funcionamiento y organización.

(…).

(…).

(…).

(…).

(…).

(…).

(…).

No obstante, en este caso particular el encargado del tratamiento, aun siendo una cuestión relativa a las nóminas, no tuvo ninguna implicación en el incidente al circunscribirse internamente al responsable.

4.- Medidas de seguridad.

4.1. Medidas previas al incidente.
Se ha requerido a la parte reclamada información sobre las medidas previas al incidente en materia de protección de datos, así como la normativa al respecto que desarrolle los protocolos de actuación.

La parte reclamada manifiesta que cuentan con las siguientes medidas técnicas y organizativas: ***(…).***

Relativo al tratamiento de datos para la gestión de nóminas, la parte reclamada manifiesta que no se ha realizado una evaluación de impacto específica, ya que interpretan que no es considerado un tratamiento que requiera esta evaluación. En consecuencia, manifiestan que tampoco se ha documentado un análisis de riesgo específico para este tratamiento: "*En lo que al tratamiento de datos relativo a la gestión de nóminas se refiere, la empresa no ha llevado a cabo una evaluación de impacto ya que, de conformidad con el artículo 35.3 del RGPD, la gestión de las nóminas no es considerado un tratamiento que requiera de esta evaluación. Asimismo, y en consecuencia con lo anterior, la empresa tampoco ha documentado un análisis del riesgo específico de este tratamiento*".

En cualquier caso, manifiestan una serie de medidas de seguridad que son de aplicación para este tratamiento. Entre ellas:

- ***(…).***
- ***(…).***
- ***(…).***
- ***(…).***
- ***(…).***
- ***(…).***
- ***(…).***
- ***(…).***

UNIQLO dispone de una plataforma digital denominada portal *ISO*. Es un portal en línea operado por la oficina de seguridad de la información del grupo corporativo, en el que se pone a disposición de los empleados los materiales y documentación relativos a seguridad de la información. Entre la documentación que se encuentra en el portal, está el mencionado reglamento básico de seguridad ("*Fast Retailing Group - Information Security Basic Regulations*") y el manual de seguridad de la información ("*Informacion Security Handbook*"). Se aporta acreditación de que dichos protocolos son accesibles dentro del portal. Como se desarrollará posteriormente, también se aporta información relativa a la difusión del uso de este portal entre los empleados.

Adicionalmente a lo expuesto, se encontrarían las medidas con el encargado del tratamiento, GM Integra RRHH S.L., aunque en este caso la brecha sería ajena a ellas.

En el marco normativo, se aporta la siguiente documentación al respecto:

- Procedimiento para la gestión de incidentes. En dicho procedimiento consta la obligación de comunicar tanto al departamento de seguridad de la información como a su responsable directo cualquier tipo de incidente, aunque no haya sido malintencionado: "*All Officers and Employees are required to report Information Security Incidents (hereinafter Incidents) to their direct manager and ISO immediately through the ISO Portal. Reporting must include actual, suspected events or anomalies with or without malicious intent*" (en castellano: "*Todos los Responsables y Empleados están obligados a notificar Incidentes de Seguridad de la Información (en adelante Incidentes) a su responsable directo y a ISO inmediatamente a través del Portal ISO. La notificación debe incluir sucesos o anomalías reales o presuntos, con o sin intención maliciosa.*").

- Reglamento básico de seguridad de la información ("*Fast Retailing Group - Information Security Basic Regulations"*). Manifiestan estaba en vigor desde febrero de 2017 y en él se hace mención a la obligación de confidencialidad que deben mantener los empleados cuando divulguen activos de información a través de medios digitales, así como la necesidad de informar en caso de pérdida de información.

- Manual de seguridad de la información ("*Informacion Security Handbook*").

- Registro de Actividades de Tratamiento, en el que consta la actividad de gestión de nóminas y los datos personales afectados por este tratamiento.

- Protocolo de protección de datos del departamento de recursos humanos. En dicho protocolo consta la necesidad de comunicar al departamento de seguridad de la información (ISO) en caso de haberse producido una brecha.

- Matriz de riesgos

- Manual para empleados de tienda

En el punto 5 de este informe se ahondará en la efectiva difusión de esta normativa entre los empleados de UNIQLO.

En relación con las medidas contractuales con el personal de recursos humanos, se aporta el Código de Conducta que se pone a disposición de los empleados en el momento de su contratación. Entre los principios que constan se encuentra el respeto a la información personal y confidencial, así como el uso indebido o inapropiado.

También se aportan las cláusulas de protección de datos para empleados. Dichas cláusulas se encuentran orientadas a los datos facilitados por el trabajador, no de cara a la gestión de datos personales de otros empleados.

4.2. Medidas adoptadas con posterioridad.
En relación con el punto anterior, se ha requerido a la parte reclamada información sobre las medidas tomadas con posterioridad al incidente, enfocadas a evitar que vuelvan a producirse sucesos de este tipo.

Manifiestan nuevamente que todas las acciones se han realizado a partir del traslado de la reclamación por parte de la AEPD, no tras producirse los hechos en agosto de 2022. Entre ellas se encuentran las siguientes:

- Apertura interna del incidente e inclusión de la brecha de seguridad en el registro de brechas de la organización. Se aporta dicho registro, donde consta el incidente junto con la matriz de riesgo asociada.

- Notificación a la AEPD, como se ha comentado previamente en el punto 2.1.

- Notificación a los afectados y al Comité de Empresa, como se ha comentado previamente en el punto 2.2.

- Contratación de servicios jurídicos externos para asesoría sobre este caso.

- Implementación de la herramienta de inteligencia de amenazas ***(...)***, que se desarrollará en el punto 6 relativo a la exfiltración de los datos.

- Revisión de los protocolos internos del departamento de recursos humanos y del proceso de envío de nóminas. Entre los cambios realizados, manifiestan: los antiguos empleados podrán descargar sus nóminas (…). Complementariamente, el departamento de recursos humanos de UNIQLO intercambiará las nóminas con la gestoría encargada de este tratamiento de manera individualizada, enviando las nóminas específicas de cada trabajador y no de manera conjunta.

A nivel de personal de la organización, manifiestan haber realizado las siguientes acciones:

- Apertura de un expediente disciplinario al empleado de recursos humanos por incumplimiento grave de los deberes de buena fe y confianza legítima al no haber seguido los protocolos existentes. Manifiestan que se considera una falta muy grave que incluso podría acarrear el despido.

- Formación a los afectados en materia de protección de datos, enfocada a la protección frente a las posibles consecuencias. Aportan correo electrónico de la convocatoria, fechada en mayo de 2023.

- Formación a los empleados de UNIQLO orientada al refuerzo sobre la protección de datos y sobre los protocolos y políticas internas de la empresa. Se proporciona un calendario tentativo de las acciones de formación.

Adicionalmente indican que se mantendrá una actitud vigilante en lo relativo a este incidente y se revisará periódicamente que los datos comprometidos no se han publicado en Internet.

Por último, aunque la parte reclamada no lo manifiesta expresamente como una medida adoptada a raíz del incidente, se destaca la adenda suscrita con la gestoría GM Integra RRHH S.L., encargada del tratamiento para los servicios de gestión de nóminas, que fue suscrita en mayo de 2023 y como se manifestó, la finalidad era reforzar la responsabilidad proactiva.

5.- Traslado de los protocolos a los empleados.
Debido a que el incidente se produjo por un error humano, resulta especialmente relevante analizar la situación y formación de los empleados en materia de protección de datos y ciberseguridad.

Se ha requerido a la parte reclamada la acreditación de la difusión y traslado de las políticas de seguridad al personal, con anterioridad a la brecha. Manifiestan al respecto que la empresa envía regularmente circulares a todos los empleados recordándoles las cuestiones relevantes desde el punto de vista de seguridad de la información y protección de datos. La parte reclamada manifiesta que el empleado en cuestión contaba con la formación necesaria para el desempeño de sus funciones, en base a lo que aporta numerosas evidencias de distinto tipo.

Se aportan las siguientes circulares de ejemplo:

- Primera circular, enviada el 20 de octubre de 2020. En esta circular el Director de seguridad de la información informa a los empleados de los aplicativos que están permitidos para el envío de información de la empresa.

- Segunda circular, del 6 de agosto de 2021, enviada también por el Director de seguridad de la información. En ella se recuerda a los empleados que la filtración de información personal constituye una violación y que los archivos que se compartan con terceros ajenos a UNIQLO deben ser enviados mediante la herramienta ***(...)***. En la circular se incluyen enlaces a la aplicación y al manual de uso.

- Tercera circular, del 26 de octubre de 2021, igualmente remitida por el mismo responsable, en ella se informa a los empleados sobre los incidentes de seguridad de la información, indicando el portal para su gestión (el mencionado portal *ISO*) y se incluye enlace al procedimiento de gestión de incidentes.

- Cuarta circular del 1 de marzo de 2022. En esta circular se ejemplifican algunas conductas contrarias a la correcta gestión de la información confidencial, como es el caso de envío información confidencial a personal no autorizado.

Para todos estos casos se acredita que el empleado involucrado de recursos humanos estaba en copia de las circulares informativas.

Por otra parte, la parte reclamada manifiesta que el empleado de recursos humanos en cuestión también recibió formación específica en materia de protección de datos vinculada a la gestión de personal. Se aportan los materiales de la formación impartida en fecha 25 de abril de 2022, dicha formación estuvo orientada a la protección de datos personales en los procesos de selección de personal.

Adicionalmente, dentro de las actividades formativas la parte reclamada manifiesta que se realiza un recordatorio anual del mencionado Código de Conducta. Se acredita que el empleado involucrado completó una formación, a fecha del 28 de enero de 2022, aunque la información proporcionada en la evidencia es escueta y no se muestra el contenido de la misma.

Otra de las actividades que manifiesta la parte reclamada que realiza es la distribución periódica de vídeos didácticos en los que se muestran los comportamientos aceptados y prohibidos de conformidad con el Código de Conducta. Se aportan dichos vídeos, en los que se tratan los códigos de conducta corporativos, buenas prácticas y manejo de información confidencial. Los vídeos son en inglés, contando con subtítulos en castellano. No se puede acreditar por la información facilitada que su efectiva difusión, ni qué personal los habría visualizado.

6.- Exfiltración de los datos afectados.

No consta que se haya producido exfiltración de los datos afectados por la brecha. La parte reclamada manifiesta que no tiene información al respecto ni que hayan podido ser utilizados para otros fines. Tal como se indica: "*el departamento de seguridad de la información, ha utilizado la herramienta de inteligencia de amenazas **(...)** para monitorizar el impacto del incidente. El resultado del análisis efectuado con esta herramienta indica que, a fecha de la presente, no se han detectado filtraciones de los datos de Uniqlo, incluyendo los datos relativos al fichero comprometido, en internet (si quiera en el conocido como" dark web")".*

Se aporta declaración del Responsable de seguridad de la información a fecha 18 de mayo de 2023, en la que se detallada el análisis realizado y las conclusiones del mismo, en el que se confirma que no se han detectado filtraciones de información ni que los datos hubieran sido publicados en contra de la voluntad de los afectados.

QUINTO: Según consta en diligencia de fecha 27 de mayo de 2024 obrante en el expediente, el volumen de negocio total anual del Grupo UNIQLO, cuya actividad económica es el comercio al por menor de prendas de vestir en establecimientos especializados, el ejercicio financiero 2023, fue de unos ***(...)***millones de euros.

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 Directora 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 las presuntas infracciones cometidas, 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 4.2) 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."

Por su parte, 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".

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 UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA realiza la recogida, consulta, comunicación por transmisión y conservación de, entre otros, los siguientes datos personales de las personas físicas que trabajan en esta empresa: nombre, dirección, número de DNI/NIE, número de la Seguridad Social, número de la cuenta bancaria, salario y su desglose, entre otros tratamientos.

UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32 del RGPD, que regula la seguridad del tratamiento.

IV
Obligación incumplida. Principios relativos al tratamiento

La letra f) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:
(…)
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

En el presente caso, con fecha 5 de agosto de 2022 la parte reclamante solicitó por correo electrónico al departamento de recursos humanos de UNIQLO que le enviasen la nómina del mes de julio (página 546 del expediente). Como respuesta, el 8 de agosto de 2022 desde UNIQLO se remitió a la parte reclamante, también por correo electrónico, un documento PDF con las nóminas de 447 de sus trabajadores, que la parte reclamante aportó junto con la reclamación.

La documentación obrante en el expediente ofrece indicios evidentes de que UNIQLO, vulneró el artículo 5.1.f) del RGPD, "*Principios relativos al tratamiento*", al no garantizar debidamente la confidencialidad e integridad de datos de carácter personal de sus trabajadores, habiéndose puesto en conocimiento de un tercero no autorizado. Este deber de confidencialidad e integridad, debe entenderse que tiene como finalidad evitar que se realicen filtraciones de datos no consentidas por los titulares de los mismos.

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 UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA, por vulneración del artículo transcrito anteriormente.

V
Tipificación y calificación de la infracción a los efectos de la prescripción del artículo 5.1.f) del RGPD

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:
a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 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 este caso, considerando la gravedad de la infracción constatada, atendiendo especialmente a las consecuencias que su comisión provoca en la parte reclamante, procede la imposición de multa, además de la adopción de medidas, en su caso.

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, la condición de gran empresa y el volumen de negocio de la parte reclamada ***(...)***millones de euros en el año 2023.

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): Al haberse enviado la información por correo electrónicos, supone un mayor riesgo de filtración de los datos, no sólo por el destinatario del correo (la parte reclamante), sino, debido a las vulnerabilidad en materia de seguridad del correo electrónico, ya que, al no estar cifrados los datos, cualquier atacante que podría acceder a los datos en tránsito. Además, el número de interesados afectados por la brecha de datos personales es de 447

- Intencionalidad/ Negligencia en la infracción (artículo 83.2, letra b), del RGPD): Aunque no se puede entender que UNIQLO actuara con dolo, se observa falta de diligencia en el cumplimiento de las obligaciones que le impone la normativa en materia de protección de datos, como es el cumplimiento y puesta en práctica de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en los tratamientos que lleva a cabo, concretamente, en la gestión de las nóminas de sus trabajadores; a este respecto puede citarse la SAN de 17/10/2007, que si bien fue dictada antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que analizamos. La sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que *"(...) el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de*

constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto

- Las categorías de los datos de carácter personal afectados por la infracción (artículo 83.2, letra g), del RGPD): Además de datos personales identificativos de los trabajadores, se filtraron datos de carácter financiero como el número de cuenta bancaria y los ingresos que perciben mensualmente. En el apartado 3.6 de las Directrices 04/2022, relativas al cálculo de las sanciones administrativas bajo el RGPD, dictadas por el Comité Europeo de Protección de Datos (en adelante, CEPD), en cumplimiento del objetivo de garantizar la aplicación coherente del Reglamento General de Protección de Datos, según le atribuye su artículo 70, se establece lo siguiente (traducción no oficial):

"*Categorías de datos personales afectados*
58. En cuanto al requisito de tener en cuenta las categorías de los datos personales afectados [artículo 83, apartado 2, letra g), del RGPD], el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por tanto, una respuesta más estricta en lo que respecta a las multas. Esto se refiere, como mínimo, a los tipos de datos a que se refieren los artículos 9 y 10 del RGPD y a los datos fuera del ámbito de aplicación de estos artículos cuya difusión provoque daños y perjuicios inmediatos al interesado 26 (por ejemplo, datos de localización, datos sobre comunicaciones privadas, números de identificación nacionales o datos financieros, como resúmenes de operaciones o números de tarjetas de crédito)."

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 76.2, letra b), de la LOPDGDD): El desarrollo de las actividades de gestión empresarial por UNIQLO requiere un tratamiento continuo de datos personales de sus trabajadores.

Además, se consideran los siguientes factores de graduación en calidad de atenuantes:

Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso (artículo 83.2, letra k), del RGPD): El mensaje de correo electrónico tenía un único destinatario, la parte reclamante.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite fijar inicialmente una sanción de multa administrativa de 300.000 € (trescientos mil euros).

VII
Obligación incumplida. Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

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

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

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

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

La documentación obrante en el expediente evidencia la vulneración del artículo 32.1 del RGPD, debido a la falta de adopción de medidas de carácter técnico y organizativas apropiadas, que posibilitó a un tercero no autorizado el acceso a los datos personales de los trabajadores de UNIQLO, que vino provocado por el envío mediante correo electrónico de las nóminas de 447 trabajadores de la empresa UNIQLO.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad al riesgo se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

En el presente caso, se evidencia que las medidas de seguridad implantadas en relación con los datos que sometía a tratamiento no eran las adecuadas para garantizar la seguridad y confidencialidad de los datos personales en el momento de producirse la quiebra.

Como señala igualmente el Considerando 39:

"…Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

Desde UNIQLO se justifican una serie de medidas técnicas y organizativas para preservar la seguridad y la privacidad de sus sistemas de información. Estas medidas no eran las adecuadas para evitar los hechos objeto de reclamación, por lo que la infracción del artículo 32 del RGPD se produce al no existir medidas que evitasen la vulneración producida. Del mismo modo, se han aportado una serie de medidas adoptadas con posterioridad, tales como permitir el acceso a los antiguos empleados a sus nóminas durante un plazo de 60 después de la terminación del contrato o la revisión del proceso de envío de nóminas por parte del departamento de recursos humanos, así como rediseñar los protocolos internos de dicho departamento. Estas medidas no pueden ser tomadas en consideración a los efectos de valorar la responsabilidad de UNIQLO en los hechos.

La responsabilidad de UNIQLO viene determinada por la brecha de datos personales puesta de manifiesto en la reclamación, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico. En este sentido, las medidas no eran apropiadas, independientemente de la brecha de datos personales producida.

La actuación negligente del empleado en la gestión de los datos personales obrantes en las nóminas de los trabajadores no exime de responsabilidad a UNIQLO. La responsabilidad de la empresa en el ámbito sancionador por la actuación negligente de un empleado que suponga el incumplimiento de la normativa de protección de datos ha sido confirmada por la jurisprudencia del Tribunal Supremo. A este respecto, cabe traer a colación la Sentencia del Tribunal Supremo núm. 188/2022 (Sala de lo Contencioso, Sección 3ª), de 15 de febrero de 2022 (rec. 7359/2020), cuyo Fundamento de Derecho Cuarto dispone: "*El hecho de que fuese la actuación negligente de una empleada no le exime de su responsabilidad en cuanto encargado de la correcta utilización de las medidas de seguridad que deberían haber garantizado la adecuada utilización del sistema de registro de datos diseñado. Como ya sostuvimos en la STS nº 196/2020, de 15 de febrero de 2021 (rec. 1916/2020) el encargado del tratamiento responde también por la actuación de sus empleados y no puede excusarse en su actuación diligente, separadamente de la actuación de sus empleados, sino que es la actuación "culpable" de éstos, consecuencia de la violación de las medidas de seguridad existentes la que fundamenta la responsabilidad de la empresa en el ámbito sancionador por actos "propios" de sus empleados o cargos, no de terceros."*
Continua la sentencia argumentando acerca de la de la responsabilidad de las personas jurídicas en nuestro ordenamiento: "…*Sencillamente sucede que, estando admitida en nuestro Derecho Administrativo la responsabilidad directa de las personas jurídicas, a las que se reconoce, por tanto, capacidad infractora, el elemento subjetivo de la infracción se plasma en estos casos de manera distinta a como sucede respecto de las personas físicas, de manera que, como señala la doctrina constitucional que antes hemos reseñado -SsTC STC 246/1991, de19 de diciembre (F.J. 2) y 129/2003, de 30 de junio (F.J. 8)- la reprochabilidad directa deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma*".

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 UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA, por vulneración del artículo transcrito anteriormente.

VIII
Tipificación y calificación de la infracción a los efectos de la prescripción del artículo 32 del RGPD

El artículo 83.4 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, se sancionará, de acuerdo con el apartado 2, con multas administrativas de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"

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 73 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:
f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679."

IX
Propuesta de sanción

De acuerdo con lo previsto en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD anteriormente transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción a imponer en el presente caso por la infracción tipificada en el artículo 32 del RGPD, tipificada en el artículo 83.4.a) del RGPD de la que se responsabiliza a UNIQLO, en una valoración inicial, se estiman concurrentes los siguientes factores:

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): Al haberse enviado la información por correo electrónicos, supone un mayor riesgo de filtración de los datos, no sólo por el destinatario del correo (la parte reclamante), sino, debido a las vulnerabilidad en materia de seguridad del correo electrónico, ya que, al no estar cifrados los datos, cualquier atacante que podría acceder a los datos en tránsito. Además, el número de interesados afectados por la brecha de datos personales es de 447

- Las categorías de los datos de carácter personal afectados por la infracción (artículo 83.2, letra g), del RGPD): Además de datos personales identificativos de los trabajadores, se filtraron datos de carácter financiero como el número de cuenta bancaria y los ingresos que perciben mensualmente. En el apartado 3.6 de las Directrices 04/2022, relativas al cálculo de las sanciones administrativas bajo el RGPD, dictadas por el Comité Europeo de Protección de Datos (en adelante, CEPD), en cumplimiento del objetivo de garantizar la aplicación coherente del Reglamento General de Protección de Datos, según le atribuye su artículo 70, se establece lo siguiente (traducción no oficial):

  "*Categorías de datos personales afectados*
  58. En cuanto al requisito de tener en cuenta las categorías de los datos personales afectados [artículo 83, apartado 2, letra g), del RGPD], el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por tanto, una respuesta más estricta en lo que respecta a las multas. Esto se refiere, como mínimo, a los tipos de datos a que se refieren los artículos 9 y 10 del RGPD y a los datos fuera del ámbito de aplicación de estos artículos cuya difusión provoque daños y perjuicios inmediatos al interesado 26 (por ejemplo, datos de localización, datos sobre comunicaciones privadas, números de identificación nacionales o datos financieros, como resúmenes de operaciones o números de tarjetas de crédito)."

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 76.2, letra b), de la LOPDGDD): El desarrollo de las actividades de gestión empresarial por UNIQLO requiere un tratamiento continuo de datos personales de sus trabajadores.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite fijar inicialmente una sanción de multa administrativa de 150.000 € (ciento cincuenta mil euros).

X
Adopción de medidas

De confirmarse la infracción, 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…", en la resolución que se adopte, se podrá requerir a UNIQLO para que en el plazo de 3 meses acredite a esta Agencia la adopción de las siguientes medidas, sin perjuicio de otras que pudieran derivarse de la instrucción del procedimiento:

- Adoptar las medidas técnicas y organizativas para garantizar la seguridad de los datos personales de sus trabajadores.

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

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora 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.

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

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a **UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA**, con NIF **W8266168G**:

- Por la presunta infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD.

- Por la presunta infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD

SEGUNDO: NOMBRAR como instructor a ***C.C.C.*** y, como secretario, a ***D.D.D.***, 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, la reclamación interpuesta por la parte reclamante y su documentación, así como, 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, sin perjuicio de lo que resulte de la instrucción, sería de multa administrativa:

- Por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) de dicha norma, multa administrativa de cuantía 300.000,00 euros
- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) de dicha norma, multa administrativa de cuantía 150.000,00 euros

QUINTO: NOTIFICAR el presente acuerdo a **UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA**, con NIF **W8266168G**, 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 360.000,00 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 360.000,00 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 270.000,00 euros.

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

A estos efectos, en caso de acogerse a alguna de ellas, deberá remitir a la Subdirección General de Inspección de datos comunicación expresa del desistimiento o renuncia a cualquier acción o recurso en vía administrativa contra la sanción indicando a cuál de las dos reducciones se acoge o si es a las dos.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (360.000,00 euros o 270.000,00 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 junto con la comunicación expresa del desistimiento o renuncia a cualquier acción o recurso en vía administrativa contra la sanción 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 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.

1479-180624
Mar España Martí
Directora de la Agencia Española de Protección de Datos
>>

SEGUNDO**:** En fecha 22 de julio de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **270000 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.

CUARTO: 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 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 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."

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

PRIMERO: DECLARAR la terminación del procedimiento **EXP202304685**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: ORDENAR a ***UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA*** 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.

TERCERO: NOTIFICAR la presente resolución a ***UNIQLO EUROPE, LTD, SUCURSAL EN ESPAÑA***.

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.

1259-16012024
Mar España Martí
Directora de la Agencia Española de Protección de Datos