- **Expediente N.º: EXP202102010**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: WALLNER EUROPA, S.L., con NIF B63809560 (en adelante, la parte reclamante o WALLNER), representada por DURÁN-SINDREÚ, ASESORES LEGALES Y TRIBUTARIOS, S.L.P., con NIF B62340716, interpuso reclamación ante la Agencia Española de Protección de Datos (AEPD) con fecha 29 de julio de 2021.

La reclamación se dirige contra ***A.A.A.*** con NIF ******NIF.1*** (en adelante, la parte reclamada).

La reclamación se funda en que la parte reclamada, exempleada de WALLNER, quien ocupaba en la empresa el puesto de coordinadora de gestores, remitió desde su cuenta de correo corporativo a su dirección personal varios correos electrónicos con documentación e información de WALLNER en la que se incluían numerosos datos personales de los que la reclamante es responsable de tratamiento.

WALLNER manifiesta que su actividad principal es la gestión de la desocupación de viviendas ocupadas por terceros sin título legítimo, por lo que, fruto de su actividad, trata datos personales de sus trabajadores, de los gestores de la desocupación de viviendas y de los ocupantes de las viviendas, "*muchos de ellos en situación de vulnerabilidad, lo que supone el tratamiento de datos de categoría especial en los términos del RGPD."*

La parte reclamante ha manifestado que tuvo constancia el 10/12/2020, día en el que la reclamada fue despedida, de que había enviado a su cuenta personal, a través de su cuenta corporativa, varios correos con documentación de la entidad el día anterior y el mismo día del despido.

En prueba de los hechos WALLNER ha aportado anexos a su reclamación algunos de los correos que la reclamada dirigió a su correo personal, así como los documentos adjuntos enviados con ellos en los que se incluían datos personales de los que ella es responsable de tratamiento. Afirma que están a disposición de la AEPD "*la totalidad de los correos desviados por la* [parte reclamada] *y de la documentación adjunta a los mismos -más de una decena de archivos- [...]"* y explica que con la reclamación ha facilitado únicamente cuatro correos debido a "*las restricciones técnicas establecidas en el trámite de presentación de denuncia ante la AEPD"* y al tamaño de los documentos adjuntos a los correos electrónicos.
La mercantil reclamante expone que los datos personales de los que ella es responsable de tratamiento que se incluían en la documentación que la extrabajadora y parte reclamada desvió a su correo personal son:

i. Datos de los gestores de Wallner: identificativos, de contacto y económicos, en particular los incentivos y comisiones que perciben.
ii. Otro tipo de información personal relativa al gestor que define su perfil profesional, como el detalle de las asignaciones de los expedientes a los gestores en función de las zonas de cobertura.
iii. Reportes de los gestores colaboradores en los que, además de zona de cobertura, se incluye el porcentaje de éxito, el coste para la Compañía, el precio medio acordado por cada uno de ellos en los expedientes que han tramitado y las entregas voluntarias acordadas y cerradas.
iv. Informes ocupacionales de viviendas con los datos identificativos y de contacto de personas ocupantes, considerados colectivos vulnerables, y direcciones de las viviendas ocupadas que pueden llegar a identificar a otros ocupantes (incluidos menores) de las viviendas tramitadas por WALLNER.
v. Datos de contacto de otros empleados de WALLNER y su firma manuscrita.
vi. Datos identificativos y de contacto de colaboradores y de clientes de WALLNER.

WALLNER subraya que la parte reclamada estaba sujeta al deber de confidencialidad y secreto en el desempeño de sus funciones, en cumplimiento de lo previsto en las cláusulas adicionales del contrato (estipulación tercera) y en el anexo al contrato de trabajo (estipulación novena), que prevén, respectivamente:

> "*Tercera. - El trabajador está obligado según circular interna a cumplir con las medidas de seguridad internas para a mantener los secretos relativos a la explotación y negocios de la empresa durante la vigencia del contrato y a su extinción. Si el trabajador incumpliere dicho deber, indemnizará a la empresa según los daños económicos causados que se irroguen, constaten o acrediten por la empresa, sin perjuicio de la responsabilidad penal que pudiera derivarse por el descubrimiento o revelación de secretos. A los efectos del presente clausulado, se entenderá por información cualquier dato existente en cualquier tipo de soporte (papel, magnético, cinta, etcétera) así como el software utilizado por la empresa, relativo a clientes, productos, precios, condiciones comerciales, así como cualquier otro de interés comercial. Cualquier información relativa a la empresa se considera secreta a todos los efectos, quedando prohibida la reproducción de la misma existente en cualquier soporte y su salida no autorizada fuera de la empresa. Cualquier documento se entenderá obtenido ilícitamente de no mediar autorización escrita de la empresa."*
>
> *"Novena." - "(…) El trabajador tiene y asume la obligación de guardar el secreto y la confidencialidad de toda la información de la empresa a la que tenga acceso durante la vigencia del presente contrato. Esta obligación subsistirá aún después de finalizada la relación laboral. El trabajador será responsable de todos los daños y perjuicios que para la empresa se deriven como consecuencia del incumplimiento doloso o culposo de dicha obligación."*

Añade que la parte reclamada, además de estar sujeta al deber de confidencialidad y secreto, en su condición de trabajadora de Wallner, estaba sujeta a la política de seguridad de la información, de la que era conocedora como el resto de los empleados, en la que se establecía que las comunicaciones por correo electrónico entre la empresa y los interlocutores debían realizarse a través del correo homologado y proporcionado por la empresa y que no estaba permitido utilizar cuentas personales

para transmitir información del negocio ni para actuaciones personales. La reclamante reproduce en su escrito los puntos 4.3, párrafo tercero, y 4.5, segundo epígrafe, punto tercero, de su política de seguridad que disponen, respectivamente:

> *"Las comunicaciones por correo electrónico entre la empresa y los interlocutores de interés deben realizarse a través del correo homologado y proporcionado por la empresa. No está permitido utilizar cuentas personales para comunicarse con los públicos de interés de la organización, para transmitir cualquier otro tipo de información del negocio, ni para hacer cualquier actuación de carácter personal."*
>
> *"Finalización de la relación laboral o cambio de puesto Wallner Europa S.L. se asegurará que todos los trabajadores, colaboradores, consultores, contratistas, terceras partes, que abandonen de la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente incluso después de finalizar la relación laboral. Gestionando así, la completa devolución de todos los activos y retirada de los derechos de acceso."*

La reclamante subraya también que estaba legitimada para analizar la cuenta de correo corporativo de la reclamada a tenor de lo estipulado en el punto 4.3, epígrafe primero, párrafos primero, segundo y tercero, de su política de seguridad y que "*Las funciones de control laboral que corresponden a la monitorización de los correos electrónicos corporativos de la extrabajadora [que, asimismo, como indica la política están limitados a un uso profesional] cumple con el deber de información previo recogido en el artículo 87 de la LOPDGDD"* siendo la base legitimadora del tratamiento la ejecución del contrato. El punto 4.3. de la política de seguridad de Wallner, epígrafe primero, dice:

> *"Wallner Europa S.L. ha asumido el compromiso de asegurar la privacidad de la información personal tratada o cedida, pues ésta se concreta en que el uso del buzón electrónico por cada trabajador debe realizarse, de forma exclusiva, dentro del ámbito de la actividad laboral. De lo descrito con anterioridad, la organización se reserva el derecho de monitorizar el acceso, para verificar el cumplimiento por el trabajador de sus deberes y obligaciones.*
> *Las comunicaciones por correo electrónico entre la empresa y los interlocutores de interés deben realizarse a través del correo homologado y proporcionado por la empresa. No está permitido utilizar cuentas personales para comunicarse con los públicos de interés de la organización, para transmitir cualquier otro tipo de información del negocio, ni para hacer cualquier actuación de carácter personal.*
> *El trabajador ha de saber que, entre otros mecanismos, se aplicarán técnicas con el fin de controlar su ordenador, incluidas las revisiones, el análisis o la monitorización remota, la indexación de la navegación por Internet, o la revisión y monitorización del correo electrónico y/o del uso de su ordenador, con el fin de cumplir con los principios de protección de datos, con y sin previo aviso, y sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones."*

Por último, la reclamante afirma que la reclamada estaba obligada a mantener la confidencialidad de los datos de carácter personal a los que accediera no solo durante la vigencia del contrato laboral sino también después de finalizado. Afirma igualmente que la reclamada ha pasado a desempeñar su trabajo en una empresa de la

competencia, por lo que podría hacer uso -uso ilegítimo- en su nuevo puesto de trabajo de esos datos personales de los que Wallner es responsable.

Adjunta a su reclamación copia de los documentos siguientes:

1.Identificados por la reclamante como documento 2:

1.1. Contrato de trabajo por tiempo indefinido en el que son partes WALLNER y la reclamada y en el que se estipula que ésta presta sus servicios como *"Coord. Red Gestores Externos".* Incluye cláusulas adicionales -1ª a 5ª- y cláusulas anexas -de la 6ª a la 11ª-. En el documento no consta ni la fecha de celebración ni la firma de la extrabajadora.

1.2. La carta de despido: escrito con el anagrama de WALLNER de fecha 10/12/2020 dirigido a la reclamada en el que pone en su conocimiento la rescisión del contrato de trabajo por despido disciplinario, con efectos a partir del 10/12/2020, con arreglo a lo estipulado en el artículo 54, puntos d) y e) del Texto Refundido del Estatuto de los Trabajadores. La empresa, tras exponer que se ha constatado la falta de interés y la disminución de rendimiento de la trabajadora, añade:

"*A pesar de lo anterior, los motivos de esta rescisión contractual tienen su origen en la vulneración del secreto de obligada reserva, [...] Lo anterior por cuanto hemos detectado que durante el día de ayer y hoy, se ha remitido desde coordinaciónred@wallnergroup.com a su correo personal* ******EMAIL.1*** *correos de contenido corporativo y con archivos cuyo contenido e información es única y exclusivamente propiedad de la Compañía Wallner Europa, S.L., y cuya divulgación posterior, impacta gravemente en la seguridad de la información de la misma.*" (El subrayado es nuestro)

En el espacio destinado a la firma de la reclamada no existe firma y aparece la indicación "*No conforme*".

1.3. Documento de liquidación y finiquito a favor de la extrabajadora y parte reclamada, de fecha 10/12/2020. En el espacio destinado a su firma aparece la leyenda "*No conforme"* y la firma de la reclamada.

1.4. Documento de autorización de remisión vía telemática del certificado de empresa al Servicio Público de Empleo Estatal de fecha 10/12/2020. En el espacio destinado a la firma de la reclamada aparece escrito *"No conforme*" y su firma.

1.5. Certificado de empresa emitido el 10/12/2020.

1.6. Documento con el anagrama de WALLNER denominado "*Devolución dispositivos personales"*, en particular "*Portátil*" y "*Móvil*", que está firmado por la reclamada el 10/12/2020.

2. Identificado por la reclamante con el número 3 aporta un documento denominado "*Política de seguridad en la información, con sus respectivos estándares",* aprobado por el Comité de Seguridad de la Información de Wallner Europa, S.L., versión 1, el 07/09/2018.

3. Identificado por la reclamante como documento número 4 aporta cuatro correos electrónicos:

3.1. Correo 1:
Enviado el 09/12/2020 desde coordinacionred@wallnergroup.com a ***EMAIL.1, con el que se envían dos archivos adjuntos: 1. Captura de pantalla con la rúbrica "*Acumulativo 03/2020 a 10/2020*", en el que se recoge diversa información organizada en columnas, entre otra, la relativa a "*Provincias", "Zona de cobertura"; "Gestor",* que incluye los nombres y los dos apellidos; "*Ingresos*"; *"Coste empresa" o "Coste empresa sin comisiones y sin gastos*".

3.2. Capturas de pantalla con información organizada en columnas siendo la primera de ellas la relativa al "*Gestor*", con el nombre y un apellido, y a la "*Dirección UR".*
Al pie del correo aparece la siguiente leyenda: "***A.A.A.***. *Coordinación Red. Parc Empresarial Cervelló. Ull de Llebre 40-42 08758 Cervelló (Barcelona) coordinacionred@wallnergroup.com".* Una leyenda idéntica consta también en los correos 2 y 3.

3.3. Correo 2:
Refleja el reenvió efectuado en fecha 10/12/2020 al correo ***EMAIL.1** desde coordinacionred@wallnergroup.com de un correo recibido en esa dirección el 18/11/2020 remitido por ***EMAIL.2** referente al asunto "*Alquileres 161120.xlsx.*" El documento anexo al citado correo contiene datos completos de numerosos domicilios con indicación de la provincia, código postal, nombre de los inquilinos y correos electrónicos de contacto.

3.4. Correo 3:
Refleja el reenvío efectuado el 10/12/2020 al correo ***EMAIL.1** desde coordinacionred@wallnergroup.com de un correo recibido en esa dirección el 5/06/2020 remitido por ***EMAIL.3** referente al asunto "*Reporte semanal gestor front y mío".* Se incluyen dos documentos anexos: 1. "Coordinación red tareas junio 2020.docx". 2. "*Reporte diario equipo front office junio 2020.xlsx*". Se incluyen dos capturas de pantalla en las que, organizadas en columnas, se recoge información relativa a las gestiones realizadas por dos gestores, identificados por su nombre y apellidos, con indicación de la fecha, el cliente, *"UR*" y la descripción de sus gestiones.

3.5. Correo 4:
Enviado el 10/12/2020 desde ***EMAIL.4** a ***EMAIL.1** con el que se envían como documentos adjuntos dos capturas de pantalla que contienen, organizada en columnas, información relativa a nombres, apellidos, DNI, empresa, puesto que ocupa esa persona, área, número de móvil, email y "*observaciones*". Encabezando el correo electrónico figura esta leyenda: "***A.A.A.*** <***EMAIL.4***> *10/12/2020 12:16 para* ***EMAIL.1**"*

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 la parte reclamada para que procediese a su análisis e informase a esta Agencia en el plazo de un mes de las

acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme al artículo 42.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), no fue recogido por la destinataria. En tal sentido, obra en el expediente la "*Certificación de imposibilidad de entrega*", emitida por la Sociedad Estatal Correos y Telégrafos, S.A. (en lo sucesivo, Correos) que certifica que el envío admitido el 07/10/2021 dirigido a la parte reclamada resultó devuelto a origen por sobrante (no recogido en oficina) el 26/10/2021, teniendo la siguiente información anexa: El 1º intento de notificación se efectuó el 14/10/2021 a las 11:56 horas, con resultado ausente. El 2º intento de notificación se efectuó el 19/10/2021, a las 18:11 horas, con resultado ausente. Se deja aviso en buzón.

TERCERO: Con fecha 11/11/2021, de conformidad con el artículo 65 de la LOPDGDD, se admite a trámite la reclamación presentada por la parte reclamante.

El acuerdo de admisión a trámite se notificó al representante de la parte reclamante por medios electrónicos en la misma fecha.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver la Directora de la Agencia Española de Protección de Datos.

II

Objeto de la reclamación y hechos acreditados

La reclamación que examinamos versa sobre la infracción de la normativa de protección de datos en la que presuntamente habría incurrido la parte reclamada, ex empleada de WALLNER, como consecuencia de haber sustraído documentación de la mercantil reclamante en la que se incluían numerosos datos de carácter personal de los que ella era responsable del tratamiento.

La documentación que WALLNER ha facilitado a la AEPD anexa a su reclamación permite estimar acreditados los siguientes hechos relevantes que delimitan la conducta de la reclamada que, a su juicio, habría vulnerado el RGPD.

1) La parte reclamada estuvo vinculada a la entidad reclamante por una relación laboral en la que ocupó el puesto de "*Coord. Red Gestores Externos*." La relación laboral se inició el 02/11/2016 y finalizó el 10/12/2020 por despido disciplinario.

2) En la carta de despido disciplinario WALLNER adujo, entre otros, los siguientes motivos:

"A pesar de lo anterior, los motivos de esta rescisión contractual tienen su origen en la vulneración del secreto de obligada reserva, [...] Lo anterior por cuanto hemos detectado que durante el día de ayer y hoy, se ha remitido desde coordinaciónred@wallnergroup.com a su correo personal ******EMAIL.1*** *correos de contenido corporativo y con archivos cuyo contenido e información es única y exclusivamente propiedad de la Compañía Wallner Europa, S.L., y cuya divulgación posterior, impacta gravemente en la seguridad de la información de la misma." (*El subrayado es nuestro)

3) WALLNER ha aportado cuatro correos electrónicos enviados desde la cuenta corporativa de la reclamada, *coordinaciónred@wallnergroup.com*, y dirigidos a su cuenta personal, ******EMAIL.1**,* con los que se incluían diversos archivos adjuntos.

En el Hecho Primero, punto 3, de esta resolución se describen con detalle los cuatro correos electrónicos enviados por la reclamada los días 09/12/2020 y 10/12/2020 desde su dirección corporativa a su dirección personal y los archivos anexos a cada uno de ellos. Cabe recordar aquí que la documentación anexa a los cuatro correos de los que se tiene noticia que la reclamada se reenvió a su cuenta particular fue la siguiente:

-Anexos al correo electrónico 1, enviado el 09/12/2020, dos archivos adjuntos:
1. Captura de pantalla con la rúbrica "*Acumulativo 03/2020 a 10/2020*", en el que se recoge diversa información, entre otra, la relativa a "*Provincias", "Zona de cobertura"; "Gestor"*, que incluye los nombres y los dos apellidos; "*Ingresos"; "Coste empresa" o "Coste empresa sin comisiones y sin gastos*".
2. Capturas de pantalla con información o relativa al "*Gestor*", con el nombre y un apellido, y a la "*Dirección UR*".

-Anexo al correo electrónico 2, enviado el 10/12/2020, el documento identificado con el nombre "*Alquileres 161120.xlsx."* que contiene datos completos de numerosos domicilios con indicación de la provincia, código postal, nombre de los inquilinos y correos electrónicos de contacto.

-Anexo al correo electrónico 3, enviado el 10/12/2020, dos documentos incluidos en un correo electrónico que recibió días antes desde la organización con el asunto "*Reporte semanal gestor front y mío".* El documento 1: "*Coordinación red tareas junio 2020.docx".* El documento 2. "*Reporte diario equipo front office junio 2020.xlsx".* Se incluyen dos capturas de pantalla en las que se recoge información relativa a las gestiones realizadas por dos gestores, identificados por su nombre y apellidos, con indicación de la fecha, el cliente, "*UR"* y la descripción de sus gestiones.

- Anexo al correo electrónico 4, enviado el 10/12/2020 dos capturas de pantalla que contienen, información relativa a nombres, apellidos, DNI, empresa, puesto que ocupa esa persona, área, número de móvil, email y “observaciones”.

4) WALLNER ha aportado diversos documentos -como las cláusulas adicionales al contrato y el anexo al contrato de trabajo- que demuestran que la parte reclamada estaba obligada en su virtud al deber de confidencialidad y secreto en el desarrollo de sus funciones.

Además, con carácter general, la política de seguridad de la empresa, a la que estaba sujeta la reclamada en su condición de empleada, le informaba sobre esta cuestión y le imponía determinadas obligaciones y prohibiciones, entre ellas, prohibía expresamente utilizar cuentas de correo particulares: “*No está permitido utilizar cuentas personales para comunicarse con los públicos de interés de la organización, para transmitir cualquier otro tipo de información del negocio, ni para hacer cualquier actuación de carácter personal.”*

La política de seguridad de WALLNER preveía, entre otras medidas, la posibilidad de analizar las cuentas de correo corporativo: *“Wallner Europa S.L. ha asumido el compromiso de asegurar la privacidad de la información personal tratada o cedida, pues ésta se concreta en que el uso del buzón electrónico por cada trabajador debe realizarse, de forma exclusiva, dentro del ámbito de la actividad laboral. De lo descrito con anterioridad, la organización se reserva el derecho de monitorizar el acceso, para verificar el cumplimiento por el trabajador de sus deberes y obligaciones*.”

5) 5) WALLNER alude a las medidas implementadas en las cláusulas de su política de seguridad:
“El trabajador ha de saber que, entre otros mecanismos, se aplicarán técnicas con el fin de controlar su ordenador, incluidas las revisiones, el análisis o la monitorización remota, la indexación de la navegación por Internet, o la revisión y monitorización del correo electrónico y/o del uso de su ordenador, con el fin de cumplir con los principios de protección de datos, con y sin previo aviso, y sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.”

III

Disposiciones aplicables

El RGPD se ocupa en su artículo 5 de los principios que presiden el tratamiento de los datos personales, precepto que dispone:

“1. Los datos personales serán:
a) tratados de manera lícita, leal y transparente con el interesado (<<licitud, lealtad y transparencia>>)
b) [...] («limitación de la finalidad»);
c) [...] («minimización de datos»);
d)[...] («exactitud»);
e) [...] («limitación del plazo de conservación»);

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»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (<<responsabilidad proactiva>>)"

El artículo 4 del RGPD, "*Definiciones*", establece que "*A efectos del presente Reglamento se entenderá por: [...]*

2)<<tratamiento>>: 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;".

IV

Inexistencia de infracción del RGPD imputable a la parte reclamada

1.De conformidad con lo establecido en el artículo 5.2 del RGPD, principio de responsabilidad proactiva, la obligación de cumplir los principios que presiden el tratamiento de datos de carácter personal establecidos en el artículo 5.1 del RGPD, así como la de estar en condiciones de demostrar su observancia, incumbe al responsable del tratamiento.

El principio de responsabilidad proactiva establecido en el artículo 5.2 del RGPD se desarrolla en el artículo 24 del RGPD, bajo la rúbrica "*Responsabilidad del responsable del tratamiento":*

"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2.Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3.La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento." (El subrayado es nuestro)

El artículo 4.7 del RGPD define la figura del «*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;"*

Entre los principios que presiden el tratamiento de datos que el responsable está obligado observar, el artículo 5.1. del RGPD menciona el de "*integridad*" (apartado f).

A propósito del principio de integridad, el artículo 32 del RGPD, "*Seguridad del tratamiento",* dispone 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 subrayado es nuestro)

El encargado de tratamiento es otro de los sujetos a quien el RGPD impone el deber de cumplir ciertas obligaciones en materia de protección de datos. El artículo 4.8 del RGPD lo define como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;"*.

La figura del encargado de tratamiento se regula en el artículo 28 del RGPD y, a tenor del punto 10 del precepto, en determinados casos podrá ser considerado responsable del tratamiento: "*Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento."*

Las Directrices 7/2020, sobre los conceptos de responsable del tratamiento y encargado de tratamiento en el RGPD, adoptadas por el Comité Europeo de Protección de Datos (CEPD) el 07/07/2021, dicen a propósito de esta última figura:

"*Para ser considerado encargado del tratamiento, es necesario reunir dos condiciones fundamentales: ser un ente independiente del responsable del tratamiento y tratar datos personales por cuenta de este.*

El encargado del tratamiento debe tratar los datos siguiendo exclusivamente las instrucciones del responsable. Aun así, las instrucciones del responsable del tratamiento pueden dejar cierto margen de discrecionalidad sobre el modo de servir mejor a los intereses de este, de modo que permitan al encargado elegir los medios técnicos y organizativos más adecuados. No obstante, si el encargado del tratamiento no se ciñe a las instrucciones del responsable y comienza a determinar sus propios fines y medios del tratamiento, estará infringiendo el RGPD. En estos casos, el encargado del tratamiento se considerará responsable en relación con dicho tratamiento y podrá ser sancionado por no haberse adherido a las instrucciones del responsable." (El subrayado es nuestro)

2.Llegados a este punto, se ha de destacar que, en el supuesto aquí planteado, la parte reclamada -empleada de la reclamante cuando ocurrieron los hechos-, no tenía la condición de responsable del tratamiento ni la de encargada de tratamiento.

La reclamada era una empleada de la mercantil reclamante y en cuanto tal, una mera usuaria de la información y documentación de WALLNER y de los datos personales que se incluían en ella, pues el acceso a esa información empresarial era necesario para el cumplimiento de sus obligaciones laborales. Ni era la responsable del tratamiento de los datos ni era un "*ente independiente*" del responsable, condición esencial para que pudiera ser considerada un encargado de tratamiento.

En definitiva, en el supuesto examinado la parte reclamada no ocupaba la posición jurídica de responsable del tratamiento ni de encargado de tratamiento, únicos sujetos que conforme al RGPD pueden ser responsables de incumplir los principios que presiden el tratamiento de los datos de carácter personal.

La parte reclamada estaba sometida a las órdenes y directrices de WALLNER, responsable de los datos personales que figuraban en sus sistemas. Las obligaciones de confidencialidad y secreteo que eran exigibles a la parte reclamada derivaban expresamente de las estipulaciones del contrato de trabajo celebrado con WALLNER -cláusulas adicionales y anexo- o bien eran consecuencia del poder de dirección del empleador concretado en la política de seguridad de la información de la empresa.

Por ello, el incumplimiento de las cláusulas del contrato suscrito con WALLNER y de la política de seguridad de la empresa en el que, según todos los indicios, parece haber incurrido la reclamada, despliega sus efectos en un ámbito ajeno al de la normativa de protección de datos de carácter personal y por tanto ajeno también a las competencias que esta AEPD tiene encomendadas. La responsabilidad en la que pudiera haber incurrido la reclamada con su conducta derivaría del incumplimiento de las obligaciones asumidas en virtud del contrato de trabajo que le vinculaba a WALLNER y debe dirimirse en ese ámbito jurídico y, si hubiera lugar a ello, en el ámbito penal.

En el supuesto analizado, en aplicación de la normativa de protección de datos de carácter personal, es WALLNER, como responsable del tratamiento de datos personales que se efectúa por sus empleados en el desempeño de la actividad empresarial que le es propia, bajo cuyas órdenes y directrices actúan, quien resultaba obligado con arreglo al RGPD a cumplir los principios de protección de datos y a acreditar su cumplimiento, entre ellos el de integridad de los datos (artículos 5.2 y 5.1.f, del RGPD)

Las Directrices 7/2020 del CEPD sobre los conceptos de responsable del tratamiento y encargado de tratamiento en el RGPD, dicen a propósito de esta cuestión:

"*19. En principio, todo tratamiento de datos personales realizado por empleados en el ámbito de las actividades de una organización se presumirá realizado bajo el control de dicha organización.", "[...] recae en la organización, en calidad de responsable del tratamiento, el deber de asegurar que se hayan aplicado medidas técnicas y organizativas apropiadas, incluyendo, p. ej., la prestación de formación e información a los empleados con vistas a garantizar el cumplimiento del RGPD."*

La documentación e información aportada por la reclamada ponen de manifiesto que WALLNER tenía implementadas medidas de carácter organizativo dirigidas a asegurar el cumplimiento del RGPD pero no se tiene conocimiento de que esa parte hubiera adoptado las *medidas técnicas apropiadas* para impedir que los documentos que contenían datos personales de cuyo tratamiento era responsable pudieran sustraerse por un empleado, incorporados como documentos anexos, mediante el envío de correos electrónicos a una cuenta ajena a la organización.

En atención a lo indicado en los párrafos precedentes, no se han encontrado evidencias que permitan responsabilizar a la parte reclamada de una infracción del RGPD.

Por lo tanto, la conducta que es objeto de la reclamación examinada queda fuera del ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a DURÁN-SINDREU, ASESORES LEGALES Y TRIBUTARIOS, S.L.P., con NIF B62340716, en su condición de representante de WALLNER EUROPA, S.L., y a ***A.A.A..***

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

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

940-110422

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