Expediente N.º: EXP202318657

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: Con fecha 13 de noviembre de 2023, se presentó reclamación con número de registro de entrada REGAGE23e00076754877 ante la Agencia Española de Protección de Datos contra **DIRECCIÓN GENERAL DE TRANSFORMACIÓN DIGITAL DE LA ADMINISTRACIÓN DE JUSTICIA** con NIF **S2813001A** (en adelante, DGTDAJ).

Los hechos que se pusieron en conocimiento de esta autoridad eran:

El reclamante, funcionario del Ministerio de Justicia, manifiesta que, para acceder al correo electrónico corporativo, además de introducir correo electrónico y contraseña, se empezó a pedir confirmación de apertura de cada sesión a través de dos opciones, a elección del usuario:

1) Enviar un mensaje confirmando que se estaba intentando acceder a la cuenta del correo desde el terminal del teléfono móvil del usuario mediante la utilización de un programa informático "******PROGRAMA.1***".

2) La segunda opción consistía en que una vez introducida en la página de inicio el nombre de la cuenta y la contraseña del usuario, se enviaba un SMS al teléfono móvil con seis dígitos que debían introducir como contraseña de inicio a la sesión de correo.

Como consecuencia de todo ello, señala que se había suministrado su teléfono móvil a alguna de las aplicaciones de ******EMPRESA.1***.

Afirma que, desde el 17 de octubre de 2023, se les comunica que, a partir del 17 de noviembre de 2023, el acceso solo se podrá hacer a través de la app ******PROGRAMA.1*** a instalar en el terminal móvil de cada usuario, obligándole a instalarse en su móvil particular una aplicación de un tercero para poder desarrollar sus funciones.

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 DGTDAJ, 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.

La notificación del traslado de la reclamación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue realizada en fecha 22 de diciembre de 2023 como consta en el acuse de recibo que obra en el expediente.

TERCERO: Con fecha 30 de enero de 2024 se recibe en esta Agencia escrito de respuesta indicando lo siguiente:

> 1. Sobre los informes técnicos o recomendaciones elaborados por el Delegado de Protección de Datos o por el responsable de seguridad, cualquiera que fuera su formato, respecto de los tratamientos sobre los que se solicita información, así como sobre las acciones posteriores adoptadas o su ausencia, derivadas de los citados informes técnicos o recomendaciones.
>
> *"Tal y como indica el reclamante se comunica por parte de la* DGTDAJ *a los usuarios que el segundo factor de autenticación no podrá efectuarse a través del número de teléfono del usuario. Esta decisión se adoptó con objeto de no utilizar datos personales de los usuarios -el número de teléfono-, principalmente respecto de aquellos que no disponen de dispositivos corporativos.*
>
> *El uso de* ******PROGRAMA.1****, con la configuración establecida, constituye una alternativa que hace innecesario el tratamiento de los datos personales del usuario. Exclusivamente se utiliza la cuenta corporativa del usuario para el funcionamiento del servicio. (…)*
>
> 2. La decisión adoptada a propósito de esta reclamación.
>
> *"Se comunicará a todos los usuarios en las formaciones generales y a través de un comunicado que no se usa ni necesita para esta cuestión el número del teléfono móvil, y que no se almacenan ningún dato personal de los usuarios en relación con esta aplicación."*
>
> 3. Sobre las causas que han motivado la incidencia que ha originado la reclamación.
>
> *"De acuerdo con lo manifestado en el punto anterior, no consideramos existencia de incidencia al objeto de la reclamación. "*

4. Sobre cualquier otra información que consideren relevante. Aportan la siguiente información:

> ***"****Requisitos de seguridad.*
> *Los sistemas de información que provee el Ministerio de Justicia, tanto directamente como mediante proveedores, a los usuarios, entre los que se incluye el reclamante en el ámbito de la Administración de Justicia, están sometidos al cumplimiento, como mínimo, de los requisitos de seguridad contenidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.*

La aplicación de este esquema es por mandato de la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y del artículo 88 del reciente Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo (art. 47 de la derogada Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia).

La mayor parte de los sistemas, por la naturaleza de la información tratada y de los servicios que se prestan a través de los mismos, principalmente en el ámbito de la Administración de Justicia, incluido el sistema de correo electrónico, son de categoría Alta, aplicándose los requisitos de seguridad correspondientes a los mecanismos de autenticación que utilizan los usuarios para verificar su identidad ante los mismos.
Entre estos requisitos se encuentra el doble factor de autenticación objeto de la reclamación, cuando el acceso se efectúa desde una zona no controlada por el Ministerio de Justicia, desde fuera de su red interna, como es el caso del usuario reclamante, extensible a su vez a los accesos habituales a través del teletrabajo. [Real Decreto 311/2022, de 3 de mayo: apartado 4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6]. (…) factor para acceso desde o a través de zonas no controladas. – [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: (…)]
*A través del sistema de *****PROGRAMA.1** se obtiene el segundo factor de autenticación complementando la contraseña que venga utilizando el usuario.*

<u>Supuesta infracción al deber de confidencialidad.</u>
No compartimos la supuesta infracción alegada por el reclamante al deber de confidencialidad en el tratamiento de datos previsto en el art. 5 de la Ley Orgánica 3/2018. Este deber de confidencialidad se refiere al art. 5.1 f) del RGPD: «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»).»

*De la instalación del *****PROGRAMA.1** y de su vinculación con la cuenta de correo corporativa del usuario no se deduce ninguna pérdida de confidencialidad de sus datos personales, no existiendo tratamiento por parte del proveedor de datos del dispositivo o del número de teléfono, que permitan identificar al usuario directa o indirectamente, tratándose exclusivamente la cuenta corporativa, dato que ya se venía tratando tanto por el Ministerio de Justicia como por el proveedor de servicios, en este caso, *****EMPRESA.1**, sin necesidad de añadir ningún dato adicional.*

La prestación del servicio por parte del proveedor recopila la información indicada más arriba, no trata datos personales de los usuarios, no vulnera su

intimidad, no efectúa una recopilación indiscreta de información, no existiendo, por otro lado, obligaciones asumidas por el usuario con (…) más allá del buen uso del sistema.

El reclamante, por otro lado, vincula la pérdida de confidencialidad de los datos de los sistemas con la mera existencia de proveedores del Ministerio de Justicia, a los que denomina "intervención de agentes externos a la Administración de Justicia", desconociendo las facultades de contratación de servicios, en este caso tecnológicos, que tienen las Administraciones Públicas, y particularmente el Ministerio de Justicia.

La disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales indica que, en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Asimismo, el Esquema Nacional de Seguridad requiere que los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público contemplen todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Desde esta perspectiva, el servicio de ******PLATAFORMA.1*** *está certificado en el Esquema Nacional de Seguridad con categoría ALTA, y en el Ministerio de Justicia se han configurado los servicios de* ******PLATAFORMA.1*** *de acuerdo con las guías de configuración segura desarrolladas por el Centro Criptológico Nacional, lo que asegura el cumplimiento de las medidas de seguridad y privacidad requeridas."*

CUARTO: Con fecha 8 de febrero de 2024, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

QUINTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

PUNTO 1. En relación con la contestación llevada a cabo por la DGTDAJ en fecha 30 de enero de 2024, se verifica que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), establece para la medida de seguridad "mecanismo de autenticación" el refuerzo R8 para todos los niveles y categorías cuando el acceso se realiza a través de zonas no controladas, citando

expresamente como ejemplo de zona no controlada el acceso a través de Internet, siendo el refuerzo R8 el Doble Factor de Autenticación (2FA) para acceso.

PUNTO 2. Con fecha 27 de marzo de 2024, la DGTDAJ ha manifestado lo siguiente:

> "*El Ministerio de Presidencia, Justicia y Relaciones con las Cortes (entonces Ministerio de Justicia), en el ámbito de la Administración de Justicia en el año 2020, con ocasión de la declaración del estado de alarma por emergencia sanitaria y la adopción de determinadas medias, entre otras, la restricción a la libertad de deambulación de las personas, dispuso la suspensión de los plazos procesales y la declaración de servicios esenciales mínimos a practicar durante tal periodo. (cfr. Disposición Adicional Segunda del Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19).*
>
> *Por tanto, desde el Ministerio se hizo todo lo posible por garantizar a la ciudadanía la prestación de estos servicios esenciales, protegiendo a su vez la integridad de todo el personal que debía atenderlos.*
>
> *El Real Decreto-ley 16/2020 de 28 de abril, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia, posteriormente tramitado como Ley 3/2020, estableció determinadas medidas en este sentido, como fue la modificación de la Disposición Adicional Quinta de la Ley 18/2011, Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.*
>
> *«Disposición adicional quinta. Dotación de medios e instrumentos electrónicos y sistemas de información.*
> *Las Administraciones competentes en materia de Justicia dotarán a todos los órganos, oficinas judiciales y fiscalías de los medios e instrumentos electrónicos y de los sistemas de información necesarios y suficientes para poder desarrollar su función eficientemente. Estos sistemas serán plenamente accesibles y operativos sin necesidad de que los usuarios se encuentren físicamente en las sedes de sus respectivos órganos, oficinas o fiscalías, con respeto a las políticas internas que garanticen el derecho a la desconexión digital recogido en el artículo 14.j.bis y en el artículo 88 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre. Asimismo, formarán a los integrantes de los mismos en el uso y utilización de dichos medios e instrumentos.»*
>
> *En cumplimiento de esta disposición, así como del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y a la vista del incremento del riesgo real de ciberataques que se estaban produciendo durante la época de pandemia, el Ministerio realizó la implantación del doble factor de autenticación, como mecanismo de refuerzo establecido en la normativa nacional de seguridad, con la finalidad de garantizar la identificación de los usuarios de los sistemas de gestión procesal.*

Ello permitió que se pudiera habilitar el trabajo a distancia del personal de la Administración de Justicia de manera segura para ellos y para los sistemas, incrementando la seguridad del uso de cuenta de usuario y contraseña en entornos o a través de redes no seguras.

En el ámbito de la Administración de Justicia tenemos, a estos efectos, tres tipos de usuarios. Dentro de las redes seguras se encuentran aquellas gestionadas por la Dirección General de Transformación Digital de la Administración de Justicia, que son aquellas que se corresponden con el ámbito territorial y de competencias del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, esto es, territorios sin competencias transferidas en materia de medios materiales y personales en Justicia y los Órganos Centrales de la Administración de Justicia (Tribunal Supremo y Audiencia Nacional)

Además, existe personal de la Administración de Justicia que depende orgánicamente del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, entre ellos, los Letrados de la Administración de Justicia, que prestan sus servicios en órganos y oficinas judiciales y fiscales en el ámbito de las Comunidades Autónomas que han asumido competencias en materia de medios personales y materiales de la Administración de Justicia. Las redes de estas Comunidades Autónomas no están dentro de las redes del Ministerio, pero gracias a un estudio de la situación conjunto con las Comunidades Autónomas, se consideran las mismas como redes seguras a estos efectos, sin que precisen utilizar el doble factor de autenticación para acceder a aplicativos del Ministerio.

Por último, en el ámbito de competencias del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, se sitúan los Juzgados de Paz, de ámbito municipal cuyos recursos materiales y personales son principalmente aportados por los Ayuntamientos que no constituyen redes seguras, siendo necesario en estos casos el acceso a los servicios de ******EMPRESA.1*** *mediante doble factor de autenticación.*

Para garantizar la seguridad de los sistemas y la protección de datos de los usuarios, se adoptó la decisión de evitar las modalidades de doble factor por medio de sms y llamada con objeto de evitar el tratamiento del dato personal del número de teléfono del usuario que no dispone de teléfono corporativo, evitando enrolamientos a través de estas modalidades, y estableciendo la instalación de ******PROGRAMA.1*** *que sólo requiere el tratamiento de la cuenta de correo corporativa del usuario y por tanto no trata ningún otro dato personal del mismo."*

PUNTO 3. Con respecto al número de usuarios de correo electrónico y número de usuarios aproximado que utiliza su móvil personal para el segundo factor de autenticación (2FA), se verifica lo siguiente:

(…)
(…)

Con respecto al número de usuarios que han expresado quejas sobre la utilización de su número de teléfono móvil personal para 2FA (cuando existía el 2FA por SMS/llamada) y sobre la solución que se adoptó en su caso con los usuarios que se quejaron o negaron a aportar sus números de teléfono particulares, la DGTDAJ indica que no existe constancia de quejas sobre la utilización del número de teléfono móvil personal.

Con respecto al número de usuarios que han expresado quejas sobre la instalación en sus terminales móviles de la aplicación ******PROGRAMA.1*** (una vez se hizo obligatoria) y la solución adoptada con los usuarios que se han quejado o negado a instalar ******PROGRAMA.1*** en sus terminales móviles particulares, la DGTDAJ ha manifestado que se abrieron 9 incidencias relacionadas con el acceso, no existiendo reclamaciones.

Solución adoptada con las incidencias:

- Cuatro de los casos se corresponden con usuarios dependientes del Ministerio de Presidencia, Justicia y Relaciones con las Cortes que trabajan en Comunidades Autónomas con competencias transferidas. En estos casos se suprimió el segundo factor de autenticación al considerar las sedes de estas Comunidades como redes seguras. Estas incidencias se resolvieron inmediatamente.

- El resto de las incidencias vienen motivadas por dificultades en la instalación de la aplicación ******PROGRAMA.1*** por cuestiones de obsolescencia del dispositivo, falta de compatibilidad y por falta de memoria en algún caso. En estos casos, temporalmente, se seguía efectuando la autenticación mediante sms. Por parte del Ministerio se está trabajando para encontrar una solución a estos casos.

PUNTO 4. Respecto a la información facilitada a los usuarios con relación al 2FA implementado previamente, así como sobre el paso obligatorio a ******PROGRAMA.1***, la DGTDAJ aporta los siguientes comunicados:

- Comunicado por correo electrónico de abril de 2021, de medidas adicionales para el acceso seguro, sobre la implementación del 2FA con dos métodos (envío de SMS y ******PROGRAMA.1***), con instrucciones a seguir.

- Dos comunicados intermedios, de octubre de 2021 y marzo de 2022 con instrucciones de cómo acceder al servicio ******PLATAFORMA.1*** desde fuera de la red interna de la Dirección General de Transformación Digital de la Administración de Justicia, y una guía de cómo configurar el 2FA, donde todavía se puede facilitar el número de teléfono del usuario para utilizar la línea telefónica (con SMS o llamada) como mecanismo de 2FA.

- Comunicado de 24 de marzo de 2022 de refuerzo de medidas de seguridad para el Espacio Digital del Ministerio, que incluye documento con instrucciones de los pasos a realizar para acceder a las aplicaciones para teletrabajo (no cita correo electrónico): *"Como refuerzo de las medidas de seguridad requeridas en el Espacio Digital, se va a mejorar el control de acceso mediante la habilitación de una segunda verificación de identidad. […]Si tiene que teletrabajar desde fuera de la oficina accediendo a Espacio*

Digital, deberá tener configurado previamente este segundo factor siguiendo los pasos de la guía adjunta. […]".

- Comunicado de 18 de julio de 2023 de refuerzo de medidas de seguridad: *"La Dirección General de Transformación Digital de la Administración de Justicia le informa que, a partir del martes 18 de julio se implantará el Doble Factor de Autenticación (MFA), para el acceso a los a los servicios en la nube de* ******EMPRESA.1*** *(****(…)****), desde fuera de la red del Ministerio de Justicia.*
El doble factor de autenticación proporciona una capa de seguridad adicional, obligando al usuario a aceptar un código de dos dígitos (segundo factor), a través de la aplicación de móvil ******PROGRAMA.1*** *(App móvil disponible en Android/iOS), antes de acceder a los servicios en la nube de* ******EMPRESA.1****.*
A partir de la fecha indicada, será necesario que se descargue la app ******PROGRAMA.1*** *en su móvil personal o corporativo y realice el registro desde la misma."*
Adjuntan manual con instrucciones para el registro y uso de la aplicación. Se verifica que en ninguno de los pasos se pide el número de teléfono del usuario. Solo se permite la utilización de ******PROGRAMA.1***. Se cita en las instrucciones que:
"Para proporcionar una capa adicional de seguridad a través de la doble autenticación, el usuario tendrá que instalarse en su móvil, ya sea corporativo o personal, la aplicación
******PROGRAMA.1****."*

PUNTO 5. Se ha solicitado un extracto o copia de la documentación contractual con ******EMPRESA.1*** (y el proveedor de suscripción de ******PLATAFORMA.1*** en su caso) aportando todas las cláusulas de Protección de Datos y de confidencialidad.

Aportan copia de los siguientes documentos, entre otros:

- Licitación nuevas ***(…).*** Acuerdo marco del sistema estatal de contratación centralizada para el suministro de servidores, sistemas de almacenamiento y software de infraestructura. Suministro suscripciones de licencias de herramientas ofimáticas, correo, aplicaciones para flujos de trabajo, análisis de datos, administración de identidades, acceso remoto, gestor de base de datos y sistema operativo, en el ámbito de la Subdirección General de Planificación y Gestión de Transformación Digital (SGPGTD). Productos basados en una solución global del fabricante ******EMPRESA.1*** para el organismo SGPGTD. Se indica que es la única que garantiza la disponibilidad inmediata, interoperabilidad de todas las soluciones del organismo y compatibilidad con los sistemas existentes.

- Licitación licencias ******EMPRESA.1*** Puesto de Usuario. Suministro de licencias para el puesto de trabajo de usuario en el ámbito del Ministerio de Justicia Lote 6 - Software de productividad y colaboración.
Se configura el proveedor como encargado del tratamiento a los efectos del REGLAMENTO (UE) 2016/679 del PARLAMENTO EUROPEO y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). Se indica que el licitador mejor clasificado aportara la declaración responsable del Anexo IV.

En el punto “12 PENALIDADES” se cita *“El incumplimiento de las medidas relativas a la seguridad de los programas en cumplimiento del ENS, o de los requisitos de seguridad para la protección de datos personales en nube tendrá la consideración de incumplimiento muy grave dando lugar a una penalidad de hasta el 10% del importe total del contrato. “*
Incluye un ANEXO III de protección de datos que estipula las categorías de interesados cuyos datos personales se tratan, categorías de datos, las finalidades del tratamiento, duración, y, como obligaciones del encargado del tratamiento incluye, entre otras, tratar los datos de acuerdo con las instrucciones del responsable, solo para la finalidad objeto del encargo, no comunicar los datos a terceras personas, garantías de subcontratación, mantener el deber de secreto, garantías de compromisos de confidencialidad de las personas autorizadas a tratar los datos, y garantías de destrucción de los datos cumplida la prestación.
Incluye Anexo IV Modelo de Declaración Responsable del cumplimiento del RGPD.

- Adjudicación: Resolución adjudicación Suministro de licencias para el puesto de trabajo de usuario.

- Oferta y Cláusulas de Protección de Datos: OFERTA TÉCNICA. Incluye una Adenda de Protección de Datos de los productos y Servicios de ******EMPRESA.1***, de 22 páginas, con un anexo a su vez de “Anexo 1: Términos de conformidad con el Reglamento General de Protección de Datos de la Unión Europea” en el que ******EMPRESA.1*** asume los compromisos dispuestos en los términos del RGPD para todos los clientes a partir del día 25 de mayo de 2018. Se indica que estos compromisos son vinculantes para ******EMPRESA.1*** con respecto al Cliente, sin importar (1) la versión de los Términos de los Productos aplicable a una concreta suscripción o licencia de Productos; o (2) cualquier otro contrato que haga referencia al presente anexo. En concreto se cita en una de las obligaciones especificadas (la 3. (b)) que ******EMPRESA.1*** *“garantizará que las personas autorizadas para tratar los Datos Personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria”.*

PUNTO 6. Sobre la ubicación de los servidores de correo electrónico utilizados.

Indican que el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes tiene provisionado su *tenant* en la Unión Europea, por lo que ******EMPRESA.1*** almacena los datos en la Unión Europea.

Se indica que un *tenant* en tecnología ******PLATAFORMA.1*** es una instancia específica de ***(…)*** que se crea cuando una organización se registra en ******PLATAFORMA.1*** con su propio dominio, y donde se incluyen todas las suscripciones y usuarios asociados a la organización, estando aislado del resto de los *tenants* de otras organizaciones a efectos de seguridad.

PUNTO 7. Sobre si se han realizado Estudios Previos o Evaluaciones de Impacto de Protección de Datos (EIPD) con carácter previo a la implantación de las soluciones de Correo Electrónico de ******EMPRESA.1*** en su organización y el 2FA. Copia de las mismas en caso afirmativo.

La parte reclamada aporta los documentos elaborados por la Oficina de Seguridad Normativa de la Dirección General de Transformación Digital de la Administración de Justicia, aclarando que, no siendo evaluaciones de impacto de protección de datos, sí que abordan aspectos puntuales sobre el tratamiento de datos personales en ***PROGRAMA.1**, y sobre la certificación de Seguridad en el ENS de ***PLATAFORMA.1** y la ubicación de sus servidores.

La DGTDAJ ha aportado el documento "Consulta sobre cumplimiento en materia de protección de datos ***PLATAFORMA.1** en la nube", en el que se indica que el servicio de ***PLATAFORMA.1** está certificado con un certificado de conformidad con el Esquema Nacional de Seguridad (ENS) con categoría ALTA. Aportan copia del certificado de conformidad con el ENS de los sistemas de información que soportan los servicios de ***PLATAFORMA.1**, de 28 de julio de 2022, renovado el 5 mayo de 2024.

Asimismo, se cita en el documento que la configuración de los servicios de ***PLATAFORMA.1** en el Ministerio de Justicia, se ha realizado siguiendo la *Guía de Seguridad de las TIC CCN-STIC 885A "Guía de configuración segura para **PLATAFORMA.1**",* y en concreto, para el servicio de correo electrónico, la *Guía CCN-STIC 885C "Guía de configuración segura para Exchange Online*", ambas desarrolladas por el Centro Criptológico Nacional, lo indican que asegura el cumplimiento de las medidas de seguridad necesarias de entre las incluidas en el ENS.

La DGTDAJ manifiesta que todo ello es para garantizar que por parte de ***EMPRESA.1** no se utilizaran más datos que aquellos que fueran estrictamente necesarios para efectuar la doble autenticación, en este caso por medio de la cuenta de correo corporativa, no recabando ningún dato personal privativo del usuario relativo a su número de teléfono.

PUNTO 8. Se ha realizado un requerimiento de información adicional, con fecha 19 de marzo de 2025, la DGTDAJ ha contestado lo siguiente:

> "Con carácter previo a dar respuesta a las cuestiones planteadas en el indicado requerimiento, hemos de manifestar una cierta extrañeza de esta Dirección General en este expediente por dos motivos principalmente.
>
> 1. El primero de ellos es que se requiere información sobre herramienta, ***PROGRAMA.1** (…), cuyo uso está extendido de forma generalizada, incluido el sector público español y europeo, como mecanismo de seguridad de doble factor de autenticación, tanto para las propias aplicaciones "en la nube" de ***EMPRESA.1** como de otros servicios y sistemas, y en su caso, la seguridad nacional.
>
> En este sentido, además, este sistema incluso cuenta con la confianza de las instituciones de la Unión Europea para sus propios empleados públicos, y que pasamos a detallar a título ejemplificativo:
>
> *1. EIOPA (European Insurance And Occupational Pensions Authority) es una institución de la Unión Europea, es la institución europea de Seguros y*

Pensiones de Jubilación. De acuerdo con su registro de actividades de tratamiento de Videoconferencia, comunicación y colaboración con ******PLATAFORMA.1****, para el tratamiento de datos personales de audio, vídeo y chat, intercambio colaborativo y redacción de documentos a través de* ******PLATAFORMA.1****, implementa Azure MultiFactor Authentication (MFA), un proceso en el que se solicita a los usuarios, tanto internos como externos, durante el proceso de inicio de sesión una forma adicional de identificación, como usar la aplicación* ******PROGRAMA.1*** *o una llamada de voz.*

2. Asimismo, ESMA (European Securities and Markets Authority) regulador y supervisor de los mercados financieros de la UE, en su registro de actividades de tratamiento relativo a ******PLATAFORMA.1****, recoge el uso de* ******PROGRAMA.1*** *para el acceso a los servicios de* ******PLATAFORMA.1*** *de nube pública proporcionado por* ******EMPRESA.1*** *en Europa.*

3. Con objeto de apoyar a los departamentos del Gobierno irlandés en la configuración de ******PLATAFORMA.1*** *para garantizar un alto nivel de seguridad y aprovechar las características y capacidades presentes en el servicio, el Centro Nacional de Seguridad Cibernética (NCSC), en coordinación con* ******EMPRESA.1*** *y (…), desarrollaron el Marco de Configuración Segura para* ******PLATAFORMA.1*** *un componente de los servicios de* ******PLATAFORMA.1****, donde se aconseja el uso de* ******PROGRAMA.1****.*

*4. También es aconsejado el uso de ***PROGRAMA.1 por parte del Banco Central de Irlanda a sus clientes.*

5. En Italia resaltamos el Consejo Regional de Calabria que, en su Normativa para el uso de servicios y herramientas informáticas, implementa la autenticación de dos factores mediante la aplicación ******PROGRAMA.1****. La instalación y la configuración se llevan a cabo de forma independiente por los usuarios en su dispositivo móvil.*

6. Por otro lado, el Manual para la gestión de la documentación y protocolo informático e identificación del Área Organizativa Homogénea del Consejo Regional del Lacio, por el que el acceso remoto a los portales se realiza a través de MFA (Multi-Factor Authentication). Los empleados deben registrar su cuenta de dominio dentro de una aplicación que genera códigos de acceso aleatorios (p. ej. ******PROGRAMA.1****, Google Authenticator). Este registro le permitirá realizar el MFA (nombre de usuario, contraseña y un token único generado aleatoriamente por la aplicación Authenticator) necesario para acceder al portal de extranet de la Región Lacio. Una vez iniciada la sesión, los empleados tendrán enlaces a recursos de información donde podrán conectarse a través de su cuenta de dominio.*

7. O incluido el Ministerio de la Salud, también lo recomienda.

8. Por último, resaltamos el gobierno de Países Bajos, que recomienda el uso de ******PROGRAMA.1****, en los resultados de la evaluación de impacto de* ******EMPRESA.1*** *(…) llevada a cabo por SURF (cooperativa de TI de las instituciones holandesas de educación e investigación), junto con el Ministerio de Justicia y Seguridad (Gestión Estratégica de Proveedores para el Gobierno Central), aunque realizada dentro de un contexto de incertidumbre sobre las transferencias internacionales a países fuera del EEE.*

[De los ocho casos aportan enlaces a sitios web con documentación al respecto].

La prohibición de la utilización de soluciones comerciales obligaría a desarrollar herramientas propias con cargo a los presupuestos públicos, lo que supondría un esfuerzo económico que muchas Administraciones no serían capaces de afrontar, poniendo en riesgo la seguridad de los sistemas.

2. Por otro lado, se pone el acento en la diferenciación entre usuarios que disponen de teléfonos corporativos, de aquellos que no, y en nuestra opinión esta interpretación no es correcta, ya que tanto los dispositivos corporativos como los personales pueden contener información personal. Es más, podría afirmarse en algunos casos, que los corporativos pudieran tener información más sensible, tanto propia como de terceros.

Como ya se indicó en escritos anteriores, esta Dirección confirmó con la empresa ******EMPRESA.1*** *los datos personales que la aplicación trataba, precisamente para evitar que se usara el número de teléfono principalmente en el caso de usuarios sin terminal corporativo, y se limitara el tratamiento a la cuenta de correo corporativa, tomando en consideración la resolución recaída en el caso del Ayuntamiento de Madrid vs Sindicato Unión de Policía Municipal (EXP202100091), que trataba el número de teléfono particular.*

En el ámbito de los sistemas de información provistos directa o indirectamente por la DGTDAJ, *afectan a un amplio espectro de colectivos de usuarios pertenecientes a responsables orgánicos y funcionales de diferentes órganos e instituciones. Las decisiones que se adoptaron para la instalación del doble factor de autenticación para el acceso a los servicios y sistemas tenían y tienen por objeto salvaguardar los datos de los ciudadanos, los datos de la Administración de Justicia, y garantizar la prestación del servicio público de Justicia como servicio esencial del Estado. Es precisamente la voluntad de blindar la seguridad de los sistemas lo que nos lleva a la implementación de estos medios.*

Buscando este objetivo, y gracias al avance de la tecnología, se eliminó el uso del número de teléfono en marzo de 2022. Y, posteriormente, desde el tercer trimestre de 2024, es posible hacer uso de certificado para autenticarse en ******PLATAFORMA.1*** *desde redes externas, estando disponible para el usuario la elección de uno u otro medio y no siendo indispensable, por tanto, el uso de* ******PROGRAMA.1****.*

Esta nueva alternativa se va ofreciendo gradualmente a los usuarios que necesitan acceder a ******PLATAFORMA.1*** *desde redes externas; debido al alto volumen de usuarios se debe acometer de forma gradual. En concreto, esta Dirección ha contactado con el reclamante, […], para informarle y ofrecerle la alternativa de uso de certificado para la autenticación, en lugar de* ******PROGRAMA.1****. Dado que, en el caso de la* ***(…)*** *y centro de trabajo del reclamante, no se dispone de acceso remoto desde esta Dirección General (el Proxy de la Diputación bloquea el acceso en remoto), se requiere asistencia técnica presencial. Además, dado que el usuario no está continuamente en la*

sede de su puesto de trabajo por diversas cuestiones, no ha sido hasta el viernes 14 de marzo que se ha podido organizar con él una mesa de trabajo con atención presencial, en la que un técnico le configuró el acceso con certificado electrónico.

No obstante lo anterior, dada la similitud con el presente caso, la naturaleza de la información a proteger, la también condición de operador crítico del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, y la decisión empresarial de implantar una app en los dispositivos móviles propios, hemos de poner de manifiesto la fundamentación jurídica que dio lugar a la Sentencia de la Sala de lo Social de la Audiencia Nacional de 29/05/2023, SAN 2644/2023 (Id Cendoj: 28079240012023100067), en conflicto colectivo contra Iberia.

«FD SEGUNDO.- […] Se pide en demanda que declaremos que: la decisión empresarial de implantar una app en los dispositivos móviles propios de los TRIPULANTES DE CABINA DE PASAJEROS supone una MODIFICACIÓN SUSTANCIAL DE LAS CONDICIONES DE TRABAJO DE CARÁCTER COLECTIVO NO JUSTIFICADA condenando a la empresa a reponerles en sus anteriores condiciones de trabajo.

FD TERCERO.- Centrados por tanto en la pretensión contenida en el suplico, la demanda debe desestimarse de plano por las razones que exponemos a continuación.

Lo actuado acredita que IBERIA oferta a los TCP un sistema alternativo de comunicación IBnet que no sustituye al que existía IBnow. Ambos permiten acceder al TCP desde dispositivos electrónicos a utilidades precisas para conocer datos referidos a su actividad laboral y sus derechos.

Por tanto, desde el momento en que el uso de IBnet es opcional y no sustitutivo de IBnow no ha existido modificación alguna de los sistemas de comunicación entre TCP y la empresa.

No consta tampoco la imposición de alguna obligación en el uso de IBnet, siendo su empleo discrecional para el trabajador.

Pero aun en el supuesto de que se determinara la necesidad de obligadamente emplear IBnet, tal medida, que no constituiría una alteración sustancial de las obligaciones laborales, sino una medida que encaja en el uso regular del poder directivo empresarial, art. 20 ET, estaría plenamente justificada por razones de seguridad informática a las que toda empresa viene obligada y más IBERIA por su condición de operador crítico en ciberseguridad, HP 4º. »

Respuesta a la información requerida

A). Sobre el Rol de ******EMPRESA.1*** y la relación contractual en relación con los servicios de la app ******PROGRAMA.1*** (***…)***, teniendo en cuenta que la aplicación ******PROGRAMA.1*** no forma parte de ******PLATAFORMA.1*** (aunque esta última se pueda configurar para usar ******PROGRAMA.1*** como segundo factor de autenticación) se piden las siguientes aclaraciones:

A.1) Roles de ***EMPRESA.1**, del Ministerio y del usuario, en relación a los tratamientos de datos personales (encargado del tratamiento/responsable), en el marco de la utilización de la aplicación ***PROGRAMA.1:

*"La Dirección General de Transformación Digital de la Administración de Justicia es la unidad responsable del tratamiento de los datos de los usuarios para que puedan acceder y utilizar los servicios online *****PLATAFORMA.1** con licencia corporativa de *****EMPRESA.1**, dadas las finalidades propias del tratamiento, incluido*****PROGRAMA.1** que tiene por objeto facilitar dicho acceso. *****EMPRESA.1** sería considerada encargada del tratamiento cuando el usuario emplea*****PROGRAMA.1** para autenticarse en los servicios online contratados.*

*En sentido similar se ha pronunciado *****EMPRESA.1**, ante la petición efectuada por esta Dirección General al objeto de esta cuestión, que se transcribe a continuación:*
*«La aplicación *****PROGRAMA.1** puede ser descargada e instalada gratuitamente por cualquier usuario. La aplicación permite al usuario autenticarse en servicios, tanto de *****EMPRESA.1** como servicios de terceros. En caso de autenticarse a un servicio de *****EMPRESA.1**, la validación se hace a través del EntraID de *****EMPRESA.1**.*
*Por consiguiente, con respecto a *****PROGRAMA.1**, es preciso distinguir dos relaciones jurídicas:*
*- Por un lado, el usuario que descarga e instala la aplicación acepta las condiciones de licencia de la aplicación. Con respecto a dicho uso, el tratamiento de datos personales se rige por las mencionadas condiciones y *****EMPRESA.1** es el responsable del tratamiento.*
*- Por otro lado, cuando el usuario emplea la aplicación para autenticarse en un servicio online contratado por su empresa o institución (en este caso, el Ministerio) bajo una licencia corporativa de *****EMPRESA.1**, el tratamiento de datos personales asociado a la autenticación y acceso al servicio online de *****EMPRESA.1** se rige por las condiciones de la licencia corporativa. Con respecto a este tratamiento, el Ministerio es el responsable y *****EMPRESA.1** es el encargado.»*

La DGTDAJ *tiene conocimiento, en todo momento, de los usuarios enrolados mediante*****PROGRAMA.1**para el acceso al servicio de *****PLATAFORMA.1** que les ofrece.*

A.2) Se ha solicitado aclaración sobre la existencia o no de un contrato de encargo del tratamiento para el uso de*****PROGRAMA.1**suscrito entre ambas partes, en el caso de que *****EMPRESA.1** actúe como encargado y el Ministerio de responsable. Se pide copia de la documentación contractual entre el Ministerio y *****EMPRESA.1**, específica para ***PROGRAMA.1, en la que conste qué tipología de datos recopila *****EMPRESA.1** y para qué finalidades:

*"El uso de *****PROGRAMA.1** constituye una de las medidas técnicas y organizativas apropiadas para el acceso a los servicios en la nube de *****PLATAFORMA.1**proporcionados asimismo por *****EMPRESA.1**, desde redes externas al Ministerio, para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de dichos sistemas, de conformidad con su categoría Alta del Esquema Nacional de Seguridad (ENS).*

Esta medida de seguridad se adopta por la DGTDAJ *como una medida necesaria dentro de su relación contractual, precisamente para garantizar la seguridad de dichos servicios contratados y la información de la* DGTDAJ *obrante en los mismos. Constituye una medida en cumplimiento de las letras c) y f) del Anexo 1: Términos de conformidad con el Reglamento General de Protección de Datos de la Unión Europea del Addendum de Protección de Datos de los Productos y Servicios de* ******EMPRESA.1****.*

Ante la petición efectuada por esta Dirección General a ******EMPRESA.1*** *al objeto de esta cuestión, se transcribe a continuación su respuesta:*

«Con respecto a la autenticación en un servicio online de ******EMPRESA.1*** *contratado por el Ministerio, como se ha indicado también, el tratamiento de datos personales se rige por las condiciones de la licencia corporativa del Ministerio, incluido el Anexo de Tratamiento de Datos (DPA), con todo lo dispuesto en él en cuanto a tipos de datos y finalidad del tratamiento. En concreto, los datos serán tratados con el propósito de validar el EntraID.»"*

A.3) Aclaración sobre el motivo por el que, si los datos recabados son para el único fin de doble factor de autenticación, se recopilan datos adicionales de registro de diagnóstico y si esos datos los conserva ******EMPRESA.1*** para sus propios fines.

La DGTDAJ transcribe la respuesta que a esta cuestión les ha facilitado ******EMPRESA.1***.:

"Los datos de diagnóstico permanecen en la aplicación hasta que, en su caso, el usuario selecciona "Enviar feedback" en la aplicación para enviar los logs a ******EMPRESA.1****. Se trata de la información necesaria para resolver el problema de la aplicación y los ingenieros de (…) únicamente los utilizan con esa finalidad."*

B). Sobre la EIPD y los riesgos.

B.1) Se ha solicitado información sobre si se ha realizado un análisis de la necesidad o no de efectuar una EIPD para el uso de la aplicación ******PROGRAMA.1.*** Copia de la documentación en caso afirmativo.

Reiteran lo manifestado en la respuesta de fecha 27 de marzo de 2024 dada al requerimiento precedente, al respecto de si se han realizado Estudios Previos o Evaluaciones de Impacto de Protección de Datos (EIPD):

Asimismo, indican que reproducen lo manifestado en su escrito de 30 de enero de 2024 en respuesta al trámite previo a la admisión a trámite de la reclamación:

"El uso de ******PROGRAMA.1****, con la configuración establecida, constituye una alternativa que hace innecesario el tratamiento de los datos personales del usuario. Exclusivamente se utiliza la cuenta corporativa del usuario para el funcionamiento del servicio (….)."*

Indican que querían garantizar que por parte de ******EMPRESA.1*** no se utilizaran más datos que aquellos que fueran estrictamente necesarios para efectuar la doble autenticación, en este caso por medio de la cuenta de correo corporativa, no

recabando ningún dato personal privativo del usuario relativo a su número de teléfono, datos identificativos del dispositivo o identificadores en línea, que pudieran permitir identificar al usuario, tal y como consta en la política de privacidad.

Manifiestan, de acuerdo con lo inmediatamente expuesto, y con la información recopilada por la aplicación, que no se consideró que el tratamiento entrañara un alto riesgo para los derechos y libertades de las personas físicas, de acuerdo con el artículo 35, apartados 1 y 3 RGPD, y no observando que el mismo constara dentro de las listas de tratamientos que requieren EIPD de la AEPD de conformidad con el apartado 4 del art. 35 del RGPD, y menos aún que hubiera dos o más criterios de la lista para realizar la EIPD, de acuerdo con lo indicado por la AEPD, *"en el momento de analizar tratamientos de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta a continuación".*

B.2) Se ha solicitado información sobre si se realizó un Análisis de Riesgos sobre la aplicación******PROGRAMA.1*** y copia de la misma en caso afirmativo, fecha y firma.

Se reiteran en lo manifestado en el punto 5 de la respuesta de fecha 27 de marzo de 2024 dada al requerimiento precedente, al respecto de si se han realizado Estudios Previos o Evaluaciones de Impacto de Protección de Datos con carácter previo a la implantación de las soluciones de Correo Electrónico de ******EMPRESA.1*** en su organización y el 2FA:

"Dada la relación contractual existente con ******EMPRESA.1****, y tras un primer análisis por parte de esta Dirección General, para garantizar un acceso desde redes externas con autenticación robusta, se optó por la aplicación de segundo factor de autenticación que ofrece el propio* ******EMPRESA.1*** *para reforzar el acceso a sus servicios. Desde la implantación del 2FA hasta la fecha se han seguido considerando los riesgos.*

En este sentido, como consecuencia del caso del Ayuntamiento de Madrid arriba indicado donde se trataba el número de teléfono particular, esta Dirección General contactó con ******EMPRESA.1*** *para profundizar en el análisis y establecer medidas para minimizar los datos personales en el uso de* ***MA.***

Asimismo, esta valoración continua con la indicada incorporación del certificado electrónico como 2FA. "

B.3) Aclaración sobre si el certificado aportado de conformidad con el Esquema Nacional de Seguridad de servicios ******EMPRESA.1*** incluye también la aplicación MA, teniendo en cuenta que no se encuentra listada en el anexo al certificado, información sobre si existen certificaciones sobre la aplicación******PROGRAMA.1*** y copia de las mismas en caso afirmativo.

Una vez solicitada aclaración a ******EMPRESA.1***, la respuesta literal es la siguiente:
"*La aplicación, como tal, no es un servicio online y, por consiguiente, el certificado de conformidad con el ENS no se aplica a ella. Los servicios online corporativos, ante los que se autentica el usuario empleando ***PROGRAMA.1, que sí están cubiertos por el certificado de conformidad con el ENS (nivel alto)."*

C). Sobre el teletrabajo, se ha solicitado confirmación del uso de la aplicación***PROGRAMA.1**para el teletrabajo. Información sobre si se contempla el uso del teléfono móvil personal del empleado en las condiciones del teletrabajo. Aportar documentación acreditativa. Número total de empleados con teletrabajo, número de empleados que acceden al teletrabajo con***PROGRAMA.1** instalado en sus teléfonos móviles particulares, y número de empleados con***PROGRAMA.1** instalado en teléfonos corporativos.

Informan que la DGTDAJ presta medios materiales, principalmente electrónicos, a los diversos colectivos de funcionarios de la Administración de Justicia, como el caso del reclamante, y es la responsable legalmente de garantizar la seguridad de la información de los ciudadanos y de los servicios que se les presta, implantando medidas de seguridad como el doble factor de autenticación en los sistemas principales, tanto los de negocio, como los prestados por ***PLATAFORMA.1**.

Indican que la DGTDAJ carece de competencias y de responsabilidades al respecto de las condiciones del teletrabajo de los diferentes cuerpos de funcionarios. Pueden confirmarse estos extremos en el Real Decreto 204/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, y se modifica el Real Decreto 1012/2022, de 5 de diciembre, por el que se establece la estructura orgánica de la Abogacía General del Estado, se regula la inspección de los servicios en su ámbito y se dictan normas sobre su personal.
(https://www.boe.es/buscar/act.php?id=BOE-A-2024-3790).

Manifiestan que los requisitos de seguridad del doble factor de autenticación son aplicables a cualquier acceso desde fuera de la red del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes (ámbito Secretaría de Estado de Justicia), como es el caso de los Juzgados de Paz y sus Agrupaciones, centro de trabajo del reclamante.

Una vez realizada esta aclaración, ofrecen los siguientes datos:
- (…).
- (…).

Manifiestan que, de todos estos empleados, no han recibido más reclamaciones que la que origina el presente expediente y que no obstante, como hemos puesto de manifiesto, para el uso del doble factor de autenticación (2FA) se eliminó la necesidad del uso del número de teléfono en marzo de 2022, y desde el tercer trimestre de 2024, es posible hacer uso de certificado electrónico para autenticarse en ***PLATAFORMA.1** desde redes externas, estando disponible para el usuario la elección de uno u otro medio y no siendo indispensable, por tanto, el uso de ***PROGRAMA.1.**

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 estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

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

II

Cuestiones previas

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

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

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

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que la DGTDAJ realiza, entre otros tratamientos, entre otros tratamientos, la recogida y conservación de datos personales de personas físicas: nombre y apellidos, fecha de nacimiento y correo electrónico.

DGTDAJ 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 citado artículo 4.7 del RGPD.

III
Licitud del tratamiento

El Artículo 6.1 "*Licitud del tratamiento*" del RGPD establece:

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

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

Por su parte el artículo 5 de la misma norma. relativo a los principios relativos al tratamiento, establecerán que los datos personales serán:
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

De forma concreta, el principio de minimización de datos, recogido en el artículo 5.1 c) del RGPD, tiene como finalidad garantizar que únicamente se traten los datos personales estrictamente necesarios para alcanzar el propósito legítimo del tratamiento, evitando la recogida o utilización de información excesiva o desproporcionada. Al reducir la cantidad de información tratada, se minimizan también los riesgos asociados a posibles accesos no autorizados, brechas de datos personales o usos indebidos.

En el presente caso, la DGTDAJ comunicó en abril de 2021 la implementación del sistema de doble factor de autenticación (2FA) como refuerzo de seguridad para el acceso para el acceso a los a los servicios en la nube de ***EMPRESA.1 desde

redes no controladas. Inicialmente, este sistema ofrecía al usuario dos métodos alternativos para completar el acceso: (1) la recepción de un código a través de SMS al teléfono móvil y (2) el uso de la aplicación ***PROGRAMA.1, instalable en dispositivos móviles, ya fueran personales o corporativos.

Posteriormente, a partir de julio de 2023, se eliminó la opción del SMS para evitar el tratamiento del número de teléfono móvil personal del usuario, estableciendo como única opción operativa el uso de ***PROGRAMA.1.

En cuanto a las implicaciones del uso de ***PROGRAMA.1, se ha confirmado que la autenticación se realiza a través de la infraestructura de ***PLATAFORMA.1 contratada mediante licencia corporativa, por lo que, en este contexto, ***EMPRESA.1 actúa como encargado del tratamiento, y no como responsable. La DGTDAJ ha aportado documentación contractual que recoge expresamente esta relación, incluyendo cláusulas de protección de datos en las que se detallan las finalidades del tratamiento, las obligaciones del encargado y las garantías en cuanto a confidencialidad, subcontratación, y seguridad. Según lo declarado por ***EMPRESA.1, cuando el usuario utiliza ***PROGRAMA.1 para acceder a servicios corporativos bajo licencia del Ministerio, los datos personales tratados se limitan a los necesarios para validar la identidad del usuario (en este caso, la cuenta de correo corporativa), sin recopilar identificadores adicionales ni información del dispositivo.

Por otra parte, la DGTDAJ ha mencionado que ya dispone de otro medio de autenticación: "*desde el tercer trimestre de 2024, es posible hacer uso de certificado electrónico para autenticarse en ***PLATAFORMA.1 desde redes externas, estando disponible para el usuario la elección de uno u otro medio y no siendo indispensable, por tanto, el uso de* ******PROGRAMA.1***".

Asimismo, ha manifestado que el reclamante ya dispone de una alternativa al uso de ******PROGRAMA.1:*** "*Esta nueva alternativa se va ofreciendo gradualmente a los usuarios que necesitan acceder a* ******PLATAFORMA.1*** *desde redes externas; debido al alto volumen de usuarios se debe acometer de forma gradual. En concreto, esta Dirección ha contactado con el reclamante, […], para informarle y ofrecerle la alternativa de uso de certificado para la autenticación, en lugar de* ******PROGRAMA.1****. Dado que, en el caso de la Agrupación de* ***(…)*** *y centro de trabajo del reclamante, no se dispone de acceso remoto desde esta Dirección General (el Proxy de la Diputación bloquea el acceso en remoto), se requiere asistencia técnica presencial. Además, dado que el usuario no está continuamente en la sede de su puesto de trabajo por diversas cuestiones, no ha sido hasta el viernes 14 de marzo que se ha podido organizar con él una mesa de trabajo con atención presencial, en la que un técnico le configuró el acceso con certificado electrónico."*

Por último, en lo relativo a la ubicación de los servidores y la posible transferencia internacional de datos, en las actuaciones de investigación se pone de manifiesto que los servicios de ******PLATAFORMA.1*** utilizados por la DGTDAJ están situados en la Unión Europea. En consecuencia, no se habría producido una transferencia internacional de datos en los términos del Capítulo V del RGPD.

IV
Conclusión

Se puede concluir que el tratamiento realizado ha sido es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, en concreto, para la finalidad legítima de garantizar la seguridad del acceso a los servicios corporativos de la DGTDAJ.

En conclusión, de los hechos descritos y la documentación obrante del expediente no se desprende que se haya producido un tratamiento de datos personales del reclamante en vulneración de la normativa de protección de datos derivado del uso de ***PROGRAMA.1** como 2FA para el acceso a la cuenta de correo corporativa.

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Por todo lo expuesto, por la Presidencia de la Agencia Española de Protección de Datos,
SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **DIRECCIÓN GENERAL DE TRANSFORMACIÓN DIGITAL DE LA ADMINISTRACIÓN DE JUSTICIA** y al reclamante.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez sea firme en vía administrativa.

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 Presidencia 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.

1245-120525

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