- Expediente N.º: EXP202100091

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: El SINDICATO UNIÓN DE POLICÍA MUNICIPAL (en lo sucesivo el reclamante), con NIF P2807900B con fecha 10/06/2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra AYUNTAMIENTO DE MADRID con NIF P2807900B (en lo sucesivo el reclamado). Los motivos en que basa la reclamación son los siguientes: el reclamante expone que el 06/05/2021 ******PUESTO.1***, envió al resto de departamentos policiales una orden jerárquica en nota interna en la que se solicitaban datos personales; de la citada nota se deduce que la intención del ******PUESTO.1*** era ceder los datos personales y los números de teléfono móvil a una empresa (***EMPRESA.1), que tiene la práctica habitual de almacenarlos en un servidor situado en un tercer país.

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), el 02/07/2021 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.

Con fecha 22/07/2021 se recibe en esta Agencia escrito de respuesta indicando que la citada nota u orden interna, como bien expresa la misma, responde a una acción generada para todo el personal del Ayuntamiento de Madrid con el objetivo de garantizar la seguridad de las comunicaciones, no es por tanto, como expresa el escrito del Sindicato, una recolección de datos con intención de ceder los mismos a una empresa, sino más bien, una acción legitimada por el mero hecho del cumplimiento de una misión realizada en interés público y en el ejercicio de poderes públicos conferidos al responsable del tratamiento, entre otros, garantizar el buen funcionamiento de los servicios públicos.

TERCERO: Con fecha 27/07/2021 la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 02/02/2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado por la presunta infracción del artículo 6.1 del RGPD, tipificada en el artículo 83.5.a) del citado RGPD.

QUINTO: Notificado el acuerdo de inicio el reclamado en fecha 16/02/2022 presentó escrito de alegaciones manifestando en síntesis lo siguiente:

- No existe en modo alguno tratamiento ilícito de datos; la nota interna es precisamente la que da transparencia a la finalidad que tiene el uso de los datos que se solicitan, explicando el origen que da lugar a la petición, el objeto, la finalidad funcional y la finalidad operativa del tratamiento.

- No cabe hablar de ilicitud del tratamiento, tal y como se expresa en el Acuerdo de inicio, toda vez que el artículo 6 del RGPD explicita en el punto 1. c) que deviene lícito el tratamiento si el mismo es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento y la citada obligación viene sustentada en la obligación de prestar el servicio público de seguridad que el Cuerpo de Policía Municipal debe prestar a los ciudadanos y que se sustenta en el Acuerdo de Junta de Gobierno de 27 de junio de 2019.

- Tampoco cabe hablar de ejecución de contrato y, mucho menos, hacia la Dirección General de Seguridad, pues de la misma no nace contrato alguno relacionado con el supuesto que nos ocupa, sino más bien una adaptación a las nuevas tecnologías, iniciada para todo el Ayuntamiento ***(…),*** cuyo modo de utilización exige un acceso securizado mediante el método identificativo del trabajador a través de número de teléfono móvil.

- No es posible la no facilitación del teléfono móvil de los funcionarios que realizan sus tareas en el ámbito funcional que precisa de las herramientas informáticas, pues supondría una paralización del servicio ***(…)*** cuyas misiones están incardinadas en el interés público y en el marco constitucional de proteger el libre ejercicio de derechos y libertades y garantizar la seguridad ciudadana.

- El informe facilitado especifica que ****EMPRESA.1* es una entidad encargada de tratamiento mediante expediente de contratación con el objetivo de modernizar el espacio de trabajo del empleado público, estableciéndose los acuerdos de encargo de tratamiento, habiendo dado su visto bueno el Delegado de Protección de Datos del Ayuntamiento, no tratándose de una cesión de datos a ****EMPRESA.1*, sino un contrato de encargo de tratamiento para la realización de determinados servicios.

- El consentimiento ha sido facilitado ***(…)***, lo cual expresa el explícito consentimiento ofrecido por los mismos mediante una acción directa, no pudiendo manifestar el reclamante que se haya obtenido el teléfono sin conocimiento de los afectados debido la publicidad abierta de la nota interna y la respuesta para poder proceder a las actualizaciones tecnológicas.

SEXTO: Con fecha 10/08/2022, se acordó la apertura de un período de práctica de pruebas, acordándose las siguientes:

> - Dar por reproducidos a efectos probatorios las reclamaciones interpuestas y su documentación, los documentos obtenidos y generados que forman parte del procedimiento E/07594/2021.

- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por el reclamado, y la documentación que a ellas acompaña.

- Solicitar al reclamado Contrato suscrito con ***EMPRESA.1 ***"(…)"*.**

En fechas 18 y 19/08/2022 el reclamado dio respuesta a la prueba practica cuyo contenido obra en el expediente.

SEPTIMO: Con fecha 29/09/2022, fue emitida Propuesta de Resolución en el sentido de que por la Directora de la Agencia Española de Protección de Datos se sancionara al reclamado por infracción del artículo del artículo 6.1 del RGPD, tipificada en el artículo 83.5.a) del citado Reglamento con sanción de apercibimiento. Asimismo, se acompañaba Anexo conteniendo la relación de los documentos obrantes en el expediente a fin de obtener copia de los que estimara convenientes.

La representación del reclamado presentó el 17/10/2022 escrito en el que alegaba en síntesis: que en el proceso de modernización y adaptación a las nuevas tecnologías emprendido por el reclamado hacía necesario incorporar sistemas de seguridad que eliminaran las amenazas externas; que el ENS determina que el responsable de seguridad establecerá los requisitos de seguridad de la información y servicios, encargándose de desarrollar la forma concreta de implementar esta seguridad por sí o a través de terceros contratados y que la estrategia se basará en las guías ENS ***(…)***, así como varias guías del CCN ***(…)*** siendo por este motivo necesario un número de teléfono móvil al que enviar notificaciones para cada acceso y autorización para registrar dicho número para este uso; que mediante Acuerdo se aprueba la política de seguridad de la información del reclamado y sus organismos, ***(…).***

OCTAVO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO. El 23/02/2021 tiene entrada en la Agencia Española de Protección de Datos escrito del reclamante manifestando que el 06/05/2021 ******PUESTO.1,*** envió al resto de departamentos policiales una orden jerárquica solicitando datos personales (número de, teléfono móvil), deduciéndose que la intención era ceder los datos personales y los números de teléfono móvil a una empresa (******EMPRESA.1***), que tiene la práctica habitual de almacenarlos en un servidor situado en un tercer país.

SEGUNDO. Consta Nota Interna de 06/05/2021 en la que se manifiesta que con motivo de la migración del correo ***(...)***, se crean buzones compartidos con el objeto de garantizar la seguridad de las comunicaciones, solicitando rellenar el Excel que se adjuntaba con los buzones que debían permanecer activos; señalando que *"Se debe tener en cuenta lo siguiente:*

1. Buzón compartido: son las cuentas genéricas de correo que se utilizan.

2. De cada cuenta genérica, indicar el Responsable con Nombre, Apellidos y Teléfono móvil.

3. El responsable tiene que asignar a Autorizados con Nombre, Apellidos y Teléfono móvil.

La solicitud del teléfono móvil a las personas autorizadas viene definida como consecuencia del requisito de seguridad que presenta dicho software, el cual utiliza para el acceso al buzón la introducción de un código que se remite mediante mensaje al teléfono móvil del usuario, como medio de verificación de su identidad, medio similar al utilizado en entidades bancarias.

Ya se ha realizado en todas las dependencias que tienen su sede en la Jefatura del Cuerpo, extendiéndose ahora al resto.

(…)"

TERCERO. Consta aportado recurso de alzada contra el escrito anterior ***(…)*** de 12/05/2021.

CUARTO. Consta escrito de respuesta del reclamado señalando la improcedencia de la interposición del recurso al no existir acto administrativo susceptible de recurso de conformidad con el artículo 112.1 de la LPACAP; también señala que la citada nota responde a una acción generada para todo el personal con el objetivo de garantizar la seguridad de las comunicaciones, acción legitimada por cumplimiento de una misión realizada en interés público y en el ejercicio de poderes públicos conferidos al responsable del tratamiento y garantizar el buen funcionamiento de los servicios públicos; que el tratamiento afectado por ésta acción corresponde a ***(…);*** que la nota se ha transmitido reglamentariamente bajo la figura del conducto reglamentario, pues se trata de una orden y que la misma contiene que para poder acceder a los elementos de trabajo como es el correo electrónico a través del buzón compartido, se precisa una clave de seguridad de carácter personal que es transmitida a través del teléfono móvil lo que garantiza tanto el acceso singularizado y autorizado, como, en su caso, parte del secreto de las comunicaciones.

QUINTO. El reclamado en escrito de 22/07/021 respondía al requerimiento de la AEPD en el mismo sentido señalado en el hecho anterior.

SEXTO. Consta aportado por el reclamado Contrato suscrito con UTE ACCENTURE-SCC ***"(…).***

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47 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 adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

II

Los hechos denunciados se concretan en el tratamiento de datos por parte del reclamado sin base legitimadora y su cesión a empresa que los almacena en un servidor situado en un tercer país, lo que podría suponer la vulneración de la normativa en materia de protección de datos.

El artículo 5 del RGPD se ocupa de los principios que han de regir el tratamiento de los datos personales. El citado precepto dispone que:

> *"1. Los datos personales serán:*
>
> *a) Tratados de manera lícita, leal y transparente con el interesado; (…)"*

Dicho tratamiento podría ser constitutivo de una infracción del artículo 6, *Licitud del tratamiento,* del RGPD en su punto 1 establece que:

"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.

(…)

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o
b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

(…)"

Por otra parte, el artículo 4 del RGPD, *Definiciones*, en sus apartados 1, 2 y 11, señala que:

"1) «datos personales»: 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;

"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;

"11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

También el artículo 6*, Tratamiento basado en el consentimiento del afectado,* de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), señala que:

"1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual".

III

1. Se imputa al reclamado una infracción del artículo 6.1 del RGPD, precepto que relaciona las distintas bases o fundamentos jurídicos en los que puede basarse el tratamiento de datos personales, siendo la concurrencia de alguno de ellos condición necesaria para respetar el principio de licitud previsto en el artículo 5.1.a) del RGPD.

De conformidad con lo establecido en el artículo 6.1 del RGPD, además del consentimiento, existen otras posibles bases que legitiman el tratamiento de datos sin necesidad de contar con la autorización de su titular, en particular, cuando sea necesario para la ejecución de un contrato en el que el afectado es parte o para la aplicación, a petición de este, de medidas precontractuales, o cuando sea 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 afectado que requieran la protección de tales datos. El tratamiento también se considera lícito cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, para proteger intereses vitales del afectado o de otra persona física o para

el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

(…)

Y en esa alegación segunda manifiesta que *"Tampoco cabe hablar de ilicitud del tratamiento, tal y como se expresa en el Acuerdo de inicio refiriendo la ilicitud del tratamiento bien en base al consentimiento, bien en la necesidad de un contrato, toda vez que el mismo artículo 6 del RGPD explicita por un lado en el punto 1 apartado c) que deviene lícito el tratamiento si el mismo es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; dicha obligación viene sustentada en la obligación de prestación de servicio público de seguridad que el Cuerpo de Policía Municipal…*

2. La cuestión fundamental que se suscita en el presente es determinar si concurre alguna de las bases legitimadoras de las recogidas en los apartados a) a f) del citado precepto, para el tratamiento de datos de carácter personal en relación con el teléfono móvil de los agentes de la policía por el reclamado.

Resulta obvio, a la luz de lo alegado por el reclamado que estas no son las relacionadas en las letras a) del artículo 6.1 del RGPD, a la que hay que añadir la que la propia norma excluye de la posibilidad de que los tratamientos realizados por las autoridades públicas en el ejercicio de sus funciones puedan tener como base jurídica de dicho tratamiento la letra f) del artículo 6.1 RGPD, esto es, el interés legítimo y, además, tampoco nos encontramos en la situación especial definida en la letra d), pues no nos encontramos ante un tratamiento para proteger un interés esencial para la vida de los interesados.

Por tanto, habría que señalar que las bases jurídicas que podrían legitimar supuestamente el tratamiento de datos por parte del Ayuntamiento son principalmente dos: la necesidad del tratamiento para el cumplimiento de una obligación legal aplicable al responsable del tratamiento definida en la letra c), o bien, la necesidad del tratamiento para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, definida en la letra e).

Al este respecto, la LOPDGDD introduce el artículo 8, relativo al *"Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos"*, que aclara cuándo el tratamiento de datos personales podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del RGPD.

Así, señala que el tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley.

Estas normas serán las encargadas de determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del RGPD.

Por otra parte, y en cuanto al tratamiento de datos personales fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable y en los términos previstos en el artículo 6.1 e) del RGPD, sólo resultará legítimo cuando derive de una competencia atribuida por una norma con rango de ley.

3. Los destinatarios del tratamiento llevado a cabo por el reclamado, como Administración pública, sean simples ciudadanos o empleados públicos, responde a la definición de responsable del tratamiento del RGPD de *"autoridad pública, servicio u otro organismo" y, por ello, estará obligada a determinar "los fines y los medios del tratamiento"* (artículo 4 7 del RGPD). Precisamente por ello, el Ayuntamiento en este caso, será el responsable del cumplimiento de los principios que se proyectan sobre el derecho a la protección de datos, pero también capaz de demostrar su cumplimiento (artículo 5.2 RGPD).

Es cierto, que en la gestión de sus recursos humanos, las Administraciones suelen hacer un uso de datos de las personas a su cargo. Podemos confirmar, que los Ayuntamientos disponen del nombre y apellido, el número de DNI, etc.

En el presente caso, se discute si con respecto a un dato personal concreto, como es el número de teléfono móvil particular ¿puede el mismo ser tratado? o por el contrario ¿su tratamiento puede considerarse como ilícito, excesivo e innecesario?

En principio, las bases de la licitud que podría esgrimir el reclamado para el tratamiento de los datos personales de los funcionarios policiales se concretan en el art. 6.1 apartado c) y e).

Y en efecto, el reclamado en escrito de 06/02/2022 ha alegado como base legitimadora del tratamiento la contenida en el apartado c) del artículo 6.1. del RGPD al manifestar que "…*deviene lícito el tratamiento si el mismo es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento…"*

El reclamado manifiesta en su escrito dicha obligación legal viene sustentada en la de prestar el servicio público de seguridad cuya competencia tiene atribuida la Policía de conformidad con las normas que se lo atribuyen.

En este sentido, la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado (en lo sucesivo LOFCS). Los Cuerpos de Seguridad del Estado se hallan divididos en tres niveles administrativos (nacional, autonómico y local).

El artículo 11 de la LOFCS establece que estas unidades tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño las siguientes funciones:

(…)
e) Mantener y restablecer, en su caso, el orden y la seguridad ciudadana.
(…)"

En segundo lugar, la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local (LBRL), en su artículo 25 establece que:

"1. El Municipio, para la gestión de sus intereses y en el ámbito de sus competencias, puede promover actividades y prestar los servicios públicos que contribuyan a satisfacer las necesidades y aspiraciones de la comunidad vecinal en los términos previstos en este artículo.

2. El Municipio ejercerá en todo caso como competencias propias, en los términos de la legislación del Estado y de las Comunidades Autónomas, en las siguientes materias:

(…)
f) Policía local, protección civil, prevención y extinción de incendios.
(…)"

Por otra parte, la Ley 1/2018, de 22 de febrero, de Coordinación de Policías Locales de la Comunidad de Madrid (LCPLCM), en su artículo 1, *Objeto*, establece que:

"1. El objeto de esta Ley es regular las funciones de coordinación de los Cuerpos de policía local en el ámbito territorial de la Comunidad de Madrid de conformidad con las competencias que le atribuyen la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, el Estatuto de Autonomía y la legislación de régimen local, así como determinar los principios, políticas e instrumentos de la seguridad pública autonómica, en el marco de la legislación vigente".

Y en lo que respecta al Ayuntamiento de Madrid, el Reglamento de la Policía Municipal del Ayuntamiento de Madrid (RPMAM), en su artículo 5, *Misiones y funciones*, señala entre otras:

"m) Realizar las funciones de protección de la seguridad ciudadana de acuerdo con la legislación vigente".

Hay que señalar que el reclamado se halla vinculado por el principio de legalidad de manera que solo puede llevar a cabo aquello para lo que el ordenamiento jurídico le permite expresamente.

Las normas citadas contienen un mandato genérico dirigido a las distintas Administraciones públicas, de la cuales forman parte los Ayuntamientos, para que

actúen en su ámbito genérico y funcional con la finalidad de mantener la seguridad pública con los medios puestos a su alcance y lograr la misión de proteger el libre ejercicio de derechos y libertades y garantizar la seguridad ciudadana.

Ahora bien, el tratamiento de datos llevado a cabo no puede ampararse en la letra c) del artículo 6.1 del RGPD ya exige que este sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, por lo que a sensu contrario, si el tratamiento no es necesario para el cumplimiento de dicha obligación el tratamiento deviene ilícito.

Y ninguna de las normas señaladas contienen precepto alguno que determine que dicho tratamiento es necesario para el cumplimiento de las mismas ni está contemplado en la LCPLCM y el RPMAM el dato de carácter personal relativo al número de teléfono móvil.

Así, en lo que se refiere al Reglamento para el Cuerpo de Policía Municipal: ni el artículo 42, *identificación profesional*, articulo 45, *expediente personal,* articulo 143, *carnet profesional,* ni en el artículo 144, *Cartera y placa policial,* contienen referencia u obligación alguna de aportar el número de telefonía móvil, como tampoco se contiene en el artículo 45, *Registro*, de la LCPLCM que establece:

"1. El Registro de policías locales dependerá y estará gestionado por la Consejería competente en materia de coordinación de policías locales. Su organización y funcionamiento se regularán reglamentariamente respetando, en todo caso, la normativa contenida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. El Registro de policías locales tiene por objeto disponer, a efectos estadísticos, de un censo de todos los miembros que integran los Cuerpos de policía local de los ayuntamientos de la Comunidad de Madrid, así como del personal de los Cuerpos que se creen al amparo de lo previsto en el artículo 53.3 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

3. El Registro de policías locales no tiene carácter público, y su acceso quedará restringido en los términos que se establezcan reglamentariamente.

4. En el Registro de policías locales deberá inscribirse el personal que integre los diversos Cuerpos de policía local de la Comunidad de Madrid así como los agentes auxiliares cualquiera que sea la denominación con que se les conozca, y en su caso el personal de los cuerpos que se creen al amparo de los previsto en el artículo 53.3 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

*La inscripción deberá contener el nombre, apellidos, fecha y lugar de nacimiento, número del Documento Nacional de Identidad y del Registro de Personal del interesado en el ayuntamiento que corresponda" (*los subrayados corresponden a la AEPD).

Por su parte, el art. 6.3 del RGPD indica que *"La finalidad del tratamiento deberá quedar determinada en dicha base jurídica"* y en el caso examinado la actividad desarrollada a la que se encuentra vinculado el tratamiento del dato de carácter personal ***(…)*** no está relacionada con los fines de la policía; el tratamiento viene determinado por el acceso a aplicaciones informáticas, el acceso al buzón compartido mediante la introducción de un código que es remitido al teléfono móvil para verificar la identidad del usuario, como cualquier otro funcionario del reclamado, dentro del proceso de modernización y adaptación a las nuevas tecnologías emprendido por el reclamado en sus distintos servicios.

En el escrito de alegaciones al acuerdo de inicio el propio reclamado manifiesta que ***(…),*** *cuyo modo de utilización exige un acceso securizado mediante el método identificativo del trabajador…"* y la Nota Interna de 06/05/2021 relativa a buzones compartidos se indica en su párrafo tercero *"Se trata de una acción generada para todo el Ayuntamiento de Madrid, con el objeto de garantizar la seguridad de las comunicaciones, …"*

Y en el mismo contrato suscrito con UTE ACCENTURE-SCC ***(…)*** se señala que:*"* ***(…)".***

Por lo tanto, tal actividad no puede estar legitimada en el cumplimiento de una obligación legal sino como bien señala en su escrito el reclamado en una adaptación a las nuevas tecnologías, ***(…).***

Así pues, estando acreditado que el reclamado ha tratado el dato del número de móvil de los agentes siendo uno de los elemento o requisito exigido por el software contratado, para el acceso al buzón compartido mediante la introducción de un código que se remite mediante mensaje al móvil del usuario, como medio de verificación de su identidad sin que este contemplado en norma alguna, no puede operar como base legitimadora del tratamiento el cumplimiento de una obligación legal (letra c, del artículo 6.1 del RGPD)

Se concluye por lo expuesto que el tratamiento de datos personales del reclamante que es objeto de valoración en el presente expediente sancionador no se amparaba en ninguna de las bases jurídicas del artículo 6.1. RGPD. Infracción del artículo 6.1 del RGPD que es subsumible en el tipo sancionador del artículo 83.5.b) del RGPD.

4. Por último, el reclamante también alegaba en su escrito de reclamación que la intención del reclamado era ceder los datos personales (incluido el número de teléfono móvil), a una empresa, ******EMPRESA.1***, que tiene como práctica habitual almacenarlos en un servidor situado en un tercer país.

No obstante, tal manifestación no puede ser compartida, hecha abstracción de lo señalado en los fundamentos anteriores de que el reclamado no cuenta con base jurídica alguna para tratar el dato del número de teléfono móvil.

El reclamado ha aportado copia del contrato celebrado con UTE ACCENTURE SCC, ******EMPRESA.1***, en cuyo Anexo XI denominado Acuerdo de Encargo del Tratamiento se establecen los acuerdos alcanzados, que además de contar con el visto bueno del Delegado de Protección de Datos, es acorde con las recomendaciones y directrices de la AEPD.

El Considerando 81 del RGPD prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento, así como del cumplimiento de la normativa de protección de datos.

(81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

El contrato suscrito con el adjudicatario incluye como no podía ser menos en el apartado sobre protección de datos y confidencialidad de la información para garantizar que el tratamiento de los datos de carácter personal y es conforme a la normativa vigente. ***(…)*** (a esta información ***EMPRESA.1 no debería acceder, aunque no hay que olvidar que es administradora del servicio por lo que podría tener acceso a los datos).

La solución de ***EMPRESA.1 licenciada cuenta con la ***(…).***

Además, el reclamado cuenta con los requisitos ***(…).***

De la misma forma, en las alegaciones al acuerdo de inicio se ha aportado certificado ***(…)*** sobre ******EMPRESA.1***.

Por tanto, no existe cesión de datos personales, sino un contrato de encargo de tratamiento para la realización de determinados servicios que aparentemente cuenta con las garantías y seguridad suficiente.

5. Por lo que respecta al servicio de correo electrónico, está basado en una plataforma ******PLATAFORMA.1***.

El Anexo III del contrato suscrito ***(…)*****,** se señala como solución la migración del correo electrónico y proporcionar dicho servicio ***(…)*** (Real Decreto 3/2010) vigente y ser conforme a la normativa de protección de datos de carácter personal.

Asimismo, se señala que ***(…)*** quien determinará, entre las soluciones de autenticación propuestas, las que considere más adecuadas y el adjudicatario las implantará en el servicio.

En este sentido, el número del teléfono móvil es uno de los elementos o requisitos de seguridad que presenta el sistema informático o software, que utiliza para el acceso al buzón compartido la introducción de un código que se remite mediante mensaje al teléfono móvil del usuario, como medio de verificación de su identidad, similar al utilizado en entidades bancarias.

La utilización de este doble factor de autenticación es un método que confirma que un usuario es quien dice ser combinando dos componentes diferentes y el método más extendido para acceder a cuentas de correo.

La implantación de este método es una forma eficaz de evitar ataques a información sensible que pueda comprometer los datos de carácter personal, además, de limitar el alcance del empleado a la información mediante el uso de dispositivos específicos y a concienciarse en el uso y manejo de buenas prácticas de seguridad.

Como bien resume el Instituto Nacional de Ciberseguridad (INCIBE) existen tres formas o familias de autenticación: 1. Algo que sabes (una contraseña) 2. Algo que tienes (un certificado, un móvil, una llave, etc.) 3. Algo que eres (biometría: huella, rostro, iris, etc.).

La necesidad de la utilización de doble factor de autenticación (algo que sabes + algo que tienes) es una comprobación de seguridad muy exigible, dificultando una posible suplantación de la identidad del usuario legítimo, ya que añade un factor más de identificación en el acceso a los datos almacenados en la instancia ***(…),*** de tal forma que aunque alguien conociera la clave de un usuario, no podría acceder al servicio al no poder verificar el código enviado por SMS o mediante llamada telefónica.

Ahora bien, en el presente caso el reclamado utiliza como uno de los elementos para lograr ese doble factor de autenticación un dato de carácter personal,

(…), para el que no está legitimado como se ha acreditado con anterioridad al no concurrir ninguna de las bases legitimadoras de las recogidas en los apartados a) a f) del artículo 6.1 del RGPD que posibilitaría el tratamiento de datos de carácter personal.

No obstante, ***(…)*** no es el único elemento que puede ser utilizado para lograr ese doble factor de autenticación, sino que como indica el INCIBE pueden ser utilizados otros elementos o factores para lograr la identificación del usuario (una tarjeta criptográfica con un certificado de empleado público, hardware o software, etc.).

El propio reclamado ha manifestado en su escrito de 19/08/2022 que: ***"(…)".***

La propia aplicación para móviles ****APLICACION.1"* puede ser utilizada para entrar en office 365 y recibir el doble factor de autenticación, ***(…)***.

IV

El reclamado en escrito de 17/10/2022 presento alegaciones a la Propuesta de Resolución señalando que el proceso de adaptación a las nuevas tecnologías hace necesario incorporar sistemas de seguridad que eliminen las amenazas externas de conformidad con las principios generales de actuación de las administraciones públicas, contenido en la Ley 40/2015, norma que señala que el ENS establece la política de seguridad en la utilización de medios electrónicos constituyendo los principios básicos y requisitos mínimos que garanticen la seguridad de la información tratada.

Hay que señalar, que nada hay que objetar a lo alegado de que en el proceso de modernización y adaptación de los servicios administrativos a las nuevas tecnologías se hace necesario amoldarse a los nuevos escenarios a fin de conseguir una administración más eficiente y eficaz, incorporando sistemas de seguridad adecuados que aborten las amenazas que puedan producirse y en este sentido la alusión al artículo 156, *Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad*, de la Ley 40/2015 se considera oportuno.

Esta misma norma ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3 la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, de manera que se garantice la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, facilitando la prestación de servicios preferentemente por dichos medios, señalando al ENS como el instrumento fundamental para el logro de dichos objetivos.

También la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, señala entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en su artículo 13, h) el relativo *"A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas".*

Por tanto, nada empece para que el expediente de contratación formalizado por el reclamado vehicule la estrategia en materia de seguridad de conformidad con los principios, requisitos y guías del ENS y del CCN para la configuración de los productos ***EMPRESA.1, así como el establecimiento del factor de doble autenticación obligatorio.

Como se señalaba con anterioridad el Anexo III del contrato suscrito ***(…)***, en consonancia con lo señalado por el reclamado en sus alegaciones se indica que:

"(…)".

Ahora bien, no es objeto del presente procedimiento determinar si el reclamado en el proceso de modernización y adaptación a las nuevas tecnologías ha adecuado su actuación a los principios generales de actuación de las administraciones públicas, contenido en la Ley 40/2015; que en lo relativo a la seguridad en la utilización de medios electrónicos se ajusta a lo señalado en el ENS o bien la utilización de guías ENS específicas para ***EMPRESA.1, como guías del CCN para la configuración de todos los productos ***EMPRESA.1 Online, así como el factor de doble autenticación obligatorio.

En el presente caso lo que se pretende dilucidar es si el reclamado ostenta habilitación legal para la utilización del dato de carácter personal controvertido, número de telefonía móvil, convirtiéndose en elemento univoco y necesario para el acceso como medio para la verificación de la identidad y validar la autenticación; cuestión está que no ha sido desvirtuada por el reclamado en sus alegaciones.

Asimismo, se ha señalado que el cumplimiento del ENS para un nivel MEDIO, los controles *"op.acc.5"* y *"op.acc.6"* obligan al uso de un segundo factor de autenticación para acceder a la información y servicios corporativos.

V

El artículo 83.5 a) del RGPD, considera que la infracción de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* es sancionable.

Por otra parte, la LOPDGDD en su artículo 72 indica: *"Infracciones consideradas muy graves:*

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)
b) El tratamiento de datos personales personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.
(…)"

VI

No obstante, el artículo 77 de la LOPDGDD, *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*, establece lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España. g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se

ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica."

En el presente caso, se aperturaba el presente procedimiento sancionador en base a la presunción de que el reclamado, ha vulnerado la normativa en materia de protección de datos de carácter personal, principio de licitud de los datos.

De conformidad con las evidencias de las que se dispone dicha conducta constituye, por parte del reclamado la infracción a lo dispuesto en el artículo 6.1 del RGPD.

Así ha quedado acreditado al tratar los datos de carácter personal de los agentes policiales, número de teléfono móvil, sin que conste que disponía de base de legitimación para ello.

Hay que señalar que el RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 77 la posibilidad de acudir a la sanción de apercibimiento y corregir los tratamientos de datos personales que no se adecúen a sus previsiones, cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica.

Asimismo, se contempla que en la resolución que se dicte se podrían establecer medidas que proceda adoptar para que cese la conducta, se corrijan los efectos de la infracción que se hubiese cometido y su adecuación a las exigencias contempladas en el artículo 6.1 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.

Se hace necesario señalar que reiterar la conducta puesta de manifiesto en la reclamación y que es causa del presente procedimiento, así como no informar seguidamente a esta AEPD de las medidas adoptadas para evitar incidencias como la señalada podría dar lugar al ejercicio de posibles actuaciones ante el responsable del tratamiento a fin de que se apliquen de manera efectiva las medidas que garanticen y no comprometan la licitud del tratamiento de los datos de carácter personal.

VII

Los poderes correctivos que el RGPD atribuye a la AEPD como autoridad de control se relacionan en su artículo 58.2, apartados a) a j).

El artículo 83.5 del RGPD fija una sanción de multa administrativa (artículo 58.2.i) para las conductas que en él se tipifican, sin perjuicio de que, como dispone el artículo 83.2. del RGPD, las multas administrativas puedan imponerse juntamente con otras medidas correctivas previstas en el artículo 58.2 del RGPD.

Al haberse confirmado la infracción, procede imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *"d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado".*

En el presente caso, se requiere al reclamado para que en el plazo de un mes a partir de la notificación de la presente resolución:

- Acredite la adopción de medidas para que no vuelvan a producirse incidencias como la que dio lugar al procedimiento sancionador: la utilización de datos de carácter personal ***(…)*** sin concurrir base legitimadora alguna de las recogidas en el artículo 6.1 del RGPD y que los tratamientos efectuados se ajustan a las disposiciones del presente Reglamento.

Se advierte que no atender el requerimiento puede ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

La Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER al AYUNTAMIENTO DE MADRID, con NIF P2807900B, por una infracción del artículo 6.1 del RGPD, tipificada en el artículo 83.5.a) del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución al AYUNTAMIENTO DE MADRID.

TERCERO: REQUERIR al AYUNTAMIENTO DE MADRID, para que en el plazo de un mes desde la notificación de esta resolución, acredite la adopción de medidas para que no vuelvan a producirse incidencias como la que dio lugar al procedimiento sancionador: la utilización del número de telefonía móvil de los agentes sin concurrir base legitimadora alguna de las recogidas en el artículo 6.1 del RGPD.

CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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