PROTOCOLO GENERAL DE ACTUACIÓN ENTRE EL MINISTERIO DEL INTERIOR Y LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS PARA LA ATENCIÓN A PERSONAS CUYOS DATOS SE HAYAN OBTENIDO Y DIFUNDIDO ILEGÍTIMAMENTE, ESPECIALMENTE EN CASO DE IMÁGENES, VÍDEOS, O AUDIOS CON DATOS SENSIBLES

En Madrid, a 24 de septiembre de 2019

REUNIDOS

De una parte, el Ministro del Interior, **D. Fernando Grande-Marlaska Gómez**, nombrado por Real Decreto 357/2018, de 6 de junio, en virtud de las competencias atribuidas por el artículo 61 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

De otra, la Directora de la Agencia Española de Protección de Datos, **Dª Mar España Martí**, nombrada por Real Decreto 715/2015, de 24 de julio (BOE nº177, de 25 de julio de 2015), en virtud de las facultades que ostenta conferidas por el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Ambas partes comparecen en nombre de las instituciones a las que respectivamente representan y, de modo recíproco, se reconocen capacidad para formalizar el presente Protocolo General de Actuación y, por ello,

EXPONEN

Primero.

Que según el artículo 1 del Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior (MIR), este Departamento es el

órgano de la Administración del Estado competente, entre otras misiones, de la preparación y ejecución de la política del Gobierno en materia de seguridad ciudadana, la promoción de las condiciones para el ejercicio de los derechos fundamentales, especialmente en relación con la libertad y la seguridad personal, en los términos establecidos en la Constitución Española y las leyes que la desarrollan, y el ejercicio del mando superior de las Fuerzas y Cuerpos de Seguridad del Estado, a los que de acuerdo con la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, se les encomienda la misión de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.

Segundo.

Que la Agencia Española de Protección de Datos (AEPD) es una autoridad administrativa independiente, con personalidad jurídica propia y plena capacidad pública y privada, que ostenta las competencias atribuidas en el 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 éstos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos -RGPD-), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD). Su principal cometido es velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación.

Corresponde a la Agencia Española de Protección de Datos ejercer las funciones establecidas en el artículo 57 del RGPD, entre las que se encuentran controlar la aplicación del Reglamento y hacerlo aplicar (artículo 57.1.a)), promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de los datos (artículo 57.1.b)), promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben (artículo 57.1.d)), facilitar información a cualquier interesado en relación con el ejercicio de sus derechos (artículo 57.1.e)), así como desempeñar cualquier otra función relacionada con la protección de los datos personales (artículo 57.1.v)).

Tercero.

Que, a pesar de sus enormes ventajas, en el ámbito de Internet y de las Tecnologías de la Información y Comunicación (TIC) tienden a reproducirse las estructuras sociales, más amplias, en las que se manifiestan las diversas formas de violencia, especialmente contra la mujer, al tiempo que aparecen otras nuevas, propias del entorno en línea. La extensión y el uso intensivo de dispositivos móviles e Internet, redes sociales y servicios como los de mensajería instantánea o de geolocalización, han servido de cauce para la proliferación de conductas violentas, comprobándose que, en muchas ocasiones, Internet y sus servicios y aplicaciones se han utilizado con la finalidad de controlar, amedrentar, acosar, humillar y chantajear a las víctimas, constituyendo un instrumento cada vez más utilizado para dichos fines.

En este sentido, las características de las TIC han dado lugar a nuevas amenazas para la mujer víctima de violencia, derivadas, entre otras, de la velocidad con la que la información se difunde en este entorno, la posibilidad de acceder a la información gracias a los motores de búsqueda y las dificultades para su eliminación. La facilidad para viralizar y la perdurabilidad en el entorno en línea entrañan nuevas situaciones de riesgo, como pueden ser el acceso y la divulgación sin consentimiento de información sensible, de fotografías o videos de carácter íntimo; la vigilancia y monitoreo de actividades en línea; daños a la reputación de la mujer; las conductas conocidas como “sextorsión” o el acoso sexual en línea.

Por todo ello, las mujeres se ven especialmente afectadas por estos fenómenos de violencia en línea, sufriendo como consecuencia daños físicos, psicológicos y económicos. En su encuesta a escala de la Unión Europea de 2014, la Agencia de Derechos Fundamentales de la UE reveló que el 23% de las mujeres había manifestado haber sufrido acoso o abuso en línea al menos una vez en su vida y que una de cada diez había sido víctima de violencia en línea.

Con la aplicación efectiva del RGPD el 25 de mayo de 2018, se pretende hacer frente a los nuevos retos que para la protección de los datos personales han planteado la rápida evolución tecnológica y la globalización derivados del aumento significativo de la magnitud de su recogida e intercambio, tal y como se expone en su Considerando segundo. En este

sentido, el RGPD amplía los derechos de los interesados, como el de supresión, de tal forma que quien haya hecho públicos datos personales y esté obligado a suprimirlos esté obligado asimismo a indicar a los responsables del tratamiento que estén tratando los mismos de la solicitud del interesado de que dichos responsables supriman cualquier enlace a ellos, o las copias o réplicas de tales datos. El principio de integridad y confidencialidad impone que los datos personales deban ser tratados de tal manera que se garantice una seguridad adecuada de éstos, 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.

Cuarto.

Los daños que provocan estas conductas contrarias a la Ley no afectan sólo a las mujeres en casos de violencia de género. La grabación y difusión de imágenes personales es uno de los instrumentos más utilizados en los casos de acoso, tanto en el entorno laboral como en el escolar -bullying y su versión a través de Internet, cyberbullying- y de acoso sexual a menores -grooming o sexting-.

En último término, toda persona, hombre o mujer, de cualquier edad, puede verse afectada por este problema. Empleando los medios que ofrece Internet han proliferado la suplantación de identidad -para cometer un fraude, o bien para construir a la víctima una reputación falseada - y el “porno vengativo”.

Igualmente, se ha extendido el conocimiento de las aplicaciones que sirven para localizar a distancia la ubicación de un dispositivo móvil, o para activar su cámara y grabar a otra persona desde otro lugar -y así poder monitorizar y controlar a la persona que lo utiliza-.

La abundancia de medios y sistemas de comunicación ha propiciado, asimismo, que los mensajes potencialmente difamatorios y los que incitan al odio se difundan a gran velocidad, de forma prácticamente instantánea.

En este contexto, es cada vez más frecuente que se publiquen en Internet imágenes, (fotografías y vídeos) y audios o documentos privados de la mujer víctima de violencia de

género, sin su consentimiento, o de los menores a su cargo, o que se difundan a través de las redes sociales contenidos de esa naturaleza, con intención vejatoria.

Ambas instituciones son conscientes de la gravedad y persistencia de estas conductas ilícitas, y de la perdurabilidad de los daños que ocasionan a las víctimas, al quedar expuesta su intimidad ante todos.

Por ello, ambos organismos coinciden en la necesidad de investigar las conductas contrarias a la Ley, y de intentar contener la expansión de esas imágenes o vídeos cuando se refieran a datos especialmente sensibles a través de Internet.

Quinto.

Conforme a lo establecido en el RGPD, sólo podrán considerarse lícitos los tratamientos de datos que se fundamenten en alguna de las bases legales definidas en su artículo 6.

Por otra parte, el RGPD, en su artículo 9.1 dispone que determinados tipos de datos personales se consideran integrantes de “categorías especiales”. Son los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Por su más profunda afectación de la intimidad de las personas y por la gravedad de los daños que puede ocasionar un tratamiento ilegítimo de aquéllos -su tratamiento inadecuado puede vulnerar otros derechos fundamentales, como el derecho a la integridad física y moral o el derecho a la no discriminación- se establece con carácter general la prohibición de su tratamiento, salvo que concurra alguno de los supuestos contemplados en el apartado 2 del citado artículo 9.

Entre los supuestos que se encuentran exceptuados de esa prohibición, cabe mencionar los siguientes:

- el consentimiento explícito otorgado por el interesado para el tratamiento de dichos datos personales (artículo 9.2.a)), y
- cuando el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos (artículo 9.2.e)).

Cuando se producen hechos de la naturaleza que se viene refiriendo en el presente documento, la Agencia Española de Protección de Datos podrá actuar si los hechos se encuentran comprendidos dentro de su ámbito de competencia.

En este punto, es necesario matizar que el tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas se encuentra excluido del ámbito de aplicación del RGPD, según lo dispuesto en su artículo 2.2 c).

Con todo, en los casos de difusión de datos sensibles a través de Internet habitualmente se realizan diferentes tipos de tratamientos, por distintos actores (personas físicas o personas jurídicas -plataformas de servicios en internet-), con diversas finalidades (actividad de negocio, o actividad sin propósito mercantil). Todos estos factores son analizados por la Agencia Española de Protección de Datos para pronunciarse sobre su competencia respecto a los casos que se plantean.

La Agencia Española de Protección de Datos es competente para asistir a las personas por falta de atención por el responsable del tratamiento en el ejercicio de los derechos reconocidos en los artículos 15 a 22 del RGPD, entre los que se encuentra el derecho de supresión -artículo 17-.

Cuando aprecia la existencia de infracción de la normativa por el responsable de un tratamiento en materia de protección de datos personales, puede incoar procedimientos sancionadores contra los responsables de tales tratamientos ilícitos de datos.

Conforme a lo dispuesto en el artículo 69 de la LOPDPGDD, en los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportase un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de

su tratamiento y, en caso de incumplirse por éstos dichos mandatos, proceder a su inmovilización. Cuando se hubiese presentado una reclamación referida a la falta de atención por un responsable de los derechos establecidos en los artículos 15 a 22 del RGPD, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento sancionador, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, sin perjuicio de la continuación del procedimiento.

Considerando que cuando una persona que sufre una situación de estas características acude a presentar una denuncia, especialmente en casos de violencia de género, puede no conocer esta función de la Agencia, ambos organismos consideran necesario reforzar la coordinación de las actuaciones entre ambos, con el fin de agilizar la atención a las víctimas.

Sexto.

Las medidas que se puedan adoptar, en el marco de la normativa de protección de datos, se han de dirigir a ayudar a aquellas personas, de cualquier sexo y edad, cuyos datos personales especialmente sensibles hayan sido tratados ilegítimamente por terceros.

La LOPDPGDD dispone en su artículo 84.2 que “la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor”.

Séptimo.

Toda estrategia de actuación debe aunar prevención y reacción. Por tanto, además de investigar y, en su caso, sancionar, las conductas infractoras, es imprescindible informar, formar y concienciar de la necesidad de proteger los datos personales.

Según se dispone en el artículo 83 de la LOPDPDGDD, el sistema educativo garantizará el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Para ello, las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la mencionada competencia digital, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red. En concordancia con lo anterior, el profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

Octavo.

Considerando todo lo anteriormente expuesto, ambas instituciones desean promover una relación intensa de colaboración, y estiman conveniente reforzar los canales de información y las acciones formativas, al objeto de poder detectar aquellos casos que presenten indicios de vulneración en materia de protección de datos. De este modo, cuando se detecten, se informaría a la persona afectada acerca de las infracciones que persigue la Agencia Española de Protección de Datos y sobre cómo presentar reclamación lo antes posible, a fin de minimizar la difusión de los contenidos en Internet y evitar un perjuicio mayor.

Por lo expuesto, las partes acuerdan suscribir el presente Protocolo General de Actuación que se regirá por las siguientes

CLÁUSULAS

Primera. *Objeto.*

El presente Protocolo General de Actuación tiene por objeto articular la colaboración entre el Ministerio del Interior y la Agencia Española de Protección de Datos para la realización de cuantas actuaciones contribuyan a incrementar la eficacia de las medidas de atención

a las personas afectadas en caso de que sus datos se hayan obtenido ilegítimamente y difundido a través de Internet, especialmente en caso de imágenes, vídeos o audios con datos sensibles, y particularmente en los casos de violencia contra la mujer.

A estos efectos, se entenderá por datos especialmente sensibles los descritos en el artículo 9.1 del RGPD.

En este marco de actuación, el MIR y la AEPD se prestarán la colaboración mutua que al efecto precisen y seguirán intensificando, con carácter institucional, sus relaciones, estableciendo iniciativas y actividades comunes dirigidas a promover la garantía de los derechos de las víctimas.

Segunda. *Aportaciones de los firmantes.*

1º. Información general sobre la AEPD.

La AEPD facilitará al MIR información sobre sus competencias y métodos de actuación. La Comisión de Seguimiento prevista en la cláusula cuarta analizará la elaboración de documentos con este propósito, a fin de que puedan ser distribuidos en las dependencias de la Policía Nacional y de la Guardia Civil para que los miembros de las Fuerzas y Cuerpos de Seguridad del Estado puedan informar a las personas que acuden a presentar denuncia.

2º. Información específica orientada a la presentación de una reclamación por parte de los afectados.

La Comisión de Seguimiento prevista en la cláusula cuarta elaborará una hoja informativa con la finalidad de que pueda estar accesible en las dependencias de la Policía Nacional y de la Guardia Civil a los efectos de que sus agentes puedan cumplir la función informativa a que se refiere el párrafo anterior, revisará ese documento periódicamente y determinará la pertinencia de elaborar otros posibles documentos o recursos para conseguir los fines indicados.

Cuando se presente denuncia ante la Policía Nacional o ante la Guardia Civil, si a raíz de los hechos que se declarasen, se detectasen indicios de conductas que vulneran la legislación en materia de protección de datos, se informará a la persona denunciante acerca de su derecho a presentar una reclamación ante la AEPD.

Se informará, asimismo, de que la reclamación que se pueda presentar ante la Agencia es gratuita.

En la Sede Electrónica de la AEPD puede cumplimentarse el formulario de reclamación. A continuación, puede enviarse electrónicamente (mediante un sistema de firma digital reconocido), o bien puede imprimirse y presentarse a través de un registro oficial en los casos en que la comunicación con la Administración no haya obligatoriamente de realizarse por vía electrónica.

3º. Información específica orientada a la presentación de una reclamación por parte de las Fuerzas y Cuerpos de Seguridad del Estado.

La Comisión de seguimiento, prevista en la cláusula cuarta, o el grupo de trabajo creado al efecto, analizará en todo caso las medidas necesarias para informar a las Fuerzas y Cuerpos de Seguridad del Estado de cómo proceder para la presentación de reclamaciones ante la AEPD y obtener evidencias que faciliten la actuación de la AEPD, en aquellos casos en los que la reclamación se presente directamente por aquéllas.

4º. Implicación de otros agentes.

La Comisión de seguimiento, prevista en la cláusula cuarta, o el grupo de trabajo que se pueda crear al efecto, promoverá la suscripción de pautas de actuación de que dispongan o puedan disponer otros agentes implicados en la utilización de medios a través de los cuales se difundan contenidos lesivos para los derechos de las personas.

5º. Programa y acciones de formación

La AEPD colaborará en los programas de formación para empleados del MIR en materia de protección de datos, singularmente en aquéllos que se dirijan específicamente a miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

Por su parte, el MIR colaborará en las acciones formativas que se desarrollen relativas a la concienciación, prevención, detección o investigación de conductas de violencia sobre la mujer.

6º. Materiales didácticos

La AEPD informará al MIR acerca de los materiales didácticos -dirigidos a las distintas etapas y niveles educativos- que se desarrollen, bien directamente por la propia AEPD, bien en el contexto de la colaboración con el Ministerio de Educación y Formación Profesional.

De este modo, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado que realicen acciones de formación y difusión en centros educativos podrán conocer estos materiales y proporcionar su referencia a la comunidad educativa.

Tercera. *Financiación.*

El presente Protocolo General de Actuación no conlleva contraprestación económica para ninguno de los firmantes, los cuales asumirán con sus propios recursos los costes de las actuaciones que, en su caso, propongan realizar, sin que se produzca en ningún caso incremento del gasto público.

Cuarta. *Medidas de control y seguimiento.*

Para el seguimiento de la ejecución del presente Protocolo General de Actuación se constituye una Comisión de Seguimiento, que estará integrada por dos representantes de cada una de las Partes, que serán designados en cada caso por las autoridades firmantes del Protocolo.

La Comisión de Seguimiento se reunirá en sesión constitutiva en el plazo de 30 días desde la entrada en vigor del Protocolo General de Actuación y determinará qué parte ejerce la función de Secretaría de la Comisión.

Esta Comisión podrá ser convocada por cualquiera de sus miembros, a efectos del oportuno seguimiento del Protocolo General de Actuación, previa indicación de los asuntos a tratar. La Comisión se reunirá cuantas veces sea preciso y, al menos, una vez al año. De cada reunión la Secretaría levantará la correspondiente acta.

La Comisión será la encargada de proponer las actuaciones y medidas a adoptar para el cumplimiento de los objetivos del Protocolo General de Actuación, los instrumentos adecuados para su ejecución y llevará a cabo su seguimiento y evaluación, con el fin de lograr las mejores condiciones para su consecución.

La Comisión adoptará los acuerdos por unanimidad, salvo que los firmantes, de común acuerdo, dispongan otra cosa. Tendrá capacidad de proponer la modificación, vigencia o resolución del Protocolo General de Actuación, dentro de lo dispuesto en el mismo. Asimismo, podrá convocar a distintas personas en razón a los asuntos a tratar y crear los grupos de trabajo que fueran necesarios para el buen cumplimiento del fin del presente Protocolo.

Las reuniones y actos de este órgano podrán realizarse telemáticamente.

Quinta. *Confidencialidad y protección de datos de carácter personal*

Los firmantes se comprometen a mantener la confidencialidad de todos los datos e informaciones facilitados por la otra parte y que sean concernientes a la ejecución del objeto del presente protocolo, debiendo ambos mantener dicha información en reserva y secreto y no revelarla de ninguna forma, total o parcialmente, a ninguna persona física o jurídica que no sea parte del mismo, salvo en los casos y mediante la forma legalmente previstos.

Si durante la ejecución del presente convenio los firmantes tratasen datos de carácter personal, éstos se obligan al cumplimiento de lo previsto en el RGPD y en la LOPDPGDD.

Sexta. *Modificación y extinción*

El presente Protocolo General de Actuación podrá ser modificado por mutuo acuerdo entre los firmantes. La modificación se incorporará como adenda al Protocolo y se considerará parte integrante del mismo.

Serán causas de resolución del presente Protocolo General de Actuación el transcurso de su plazo de vigencia sin haberse acordado su prórroga, el mutuo acuerdo de las partes o la concurrencia de causa de fuerza mayor que imposibilite el objeto de dicho Protocolo.

Séptima. *Legislación aplicable*

El presente Protocolo se regirá por lo establecido en él, y subsidiariamente, por lo dispuesto en la Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público, en lo que le resulte aplicable.

La resolución de cualquier discrepancia que pudiera surgir en la interpretación, ejecución o cumplimiento del Protocolo General de Actuación se llevará a cabo en el seno de la Comisión de Seguimiento

El presente Protocolo no es jurídicamente vinculante ni supone la formalización de compromisos jurídicos concretos y exigibles entre las partes.

Octava. *Inicio de la aplicación y duración.*

Este Protocolo General de Actuación resultará eficaz desde la fecha de su firma y su periodo de duración será de cuatro años, pudiendo prorrogarse por mutuo acuerdo expreso de las partes antes de su finalización, mediante adenda, por otro período de hasta cuatro años.

Y en prueba de conformidad de cuanto antecede, firman el presente Protocolo General de Actuación en dos ejemplares originales, igualmente válidos, en el lugar y la fecha arriba indicadas.

POR EL MINISTERIO DEL INTERIOR	POR LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
Fernando Grande-Marlaska Gómez	Mar España Martí