8. MEMORIA DEL DELEGADO DE PROTECCIÓN DE DATOS DEL MINISTERIO FISCAL

8.1 **Introducción**

Una de las principales actuaciones realizadas por el Delegado de Protección de Datos del Ministerio Fiscal (DPD) en el año 2022 fue la elaboración y posterior difusión, en el mes de junio, de la «Guía Básica de actuaciones a desarrollar por las Fiscalías, Órganos y Unidades del Ministerio Fiscal en materia de protección de datos» llevada a cabo con el fin de informar y asesorar al Ministerio Fiscal, como responsable del tratamiento (por medio de las jefaturas de sus fiscalías, órganos y unidades) y a la plantilla de fiscales y de funcionarios de las obligaciones que les incumben en esta materia así como para que fueran corregidas ciertas deficiencias en la implementación de la normativa de protección de datos que habían sido detectadas a raíz de diversas actuaciones de supervisión.

El objetivo de la referida Guía no es la de suplir ni simplificar la normativa vigente o las instrucciones que en esta materia se impartan por la Fiscalía General del Estado o por las administraciones prestacionales en su ámbito competencial (fundamentalmente, en este caso, en lo que se refiere a la seguridad de la información) a cuyo conocimiento y cumplimiento están obligados todos los miembros del Ministerio Fiscal y los componentes de la oficina fiscal, sino que tiene por finalidad facilitar la aplicación efectiva de la misma en el desarrollo de la labor cotidiana de las fiscalías y concienciar en la cultura de protección de datos.

A su vez, dicha Guía tiene por objeto reflejar los aspectos que serán objeto de los procesos de verificación y supervisión del cumplimiento de la normativa de protección de datos que se lleven a cabo.

Dicho documento, al plasmar actuaciones básicas, tiene cierta vocación de perdurabilidad, no obstante podrá ser objeto de correcciones, modificaciones y actualizaciones cuando así se estime preciso con el fin de adaptarla a las exigencias que se puedan derivar de nueva normativa, de instrucciones emanadas de la Fiscalía General del Estado o aquellas que se fijen por medio de la PSIJE (Política de Seguridad de la Información Judicial Electrónica), así como de las recomendaciones o indicaciones que se efectúen por el DPD del MF.

En cualquier caso, en el mismo ya se incorporaron en uno de sus anexos diversas notas internas emitidas por el DPD en las que se recogen recomendaciones, pautas e indicaciones sobre diversas cuestio-

nes, siendo este el modo en el que también se irá complementando en el futuro.

El art. 22.1 del Real Decreto 305/2022, de 3 de mayo, *por el que se aprueba el Reglamento del Ministerio Fiscal* (RMF) dispone que el Ministerio Fiscal, dentro del marco de sus competencias y de conformidad con la normativa de aplicación, es el responsable del tratamiento de datos personales que realice en el ejercicio de sus funciones, a su vez la Instrucción FGE 2/2019 *sobre protección de datos en el ámbito del Ministerio Fiscal* establece que la determinación del Ministerio Fiscal como responsable del tratamiento en el estricto ámbito de sus competencias supone que las obligaciones que le impone la normativa de protección de datos también se ejercen a través de las jefaturas de los órganos fiscales, unidades y fiscalías que llevan a cabo actividades de tratamiento puesto que su dirección y organización se ejerce en representación del Ministerio Fiscal (arts. 2.1 y 22 EOMF).

El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la oficina fiscal, se rigen por lo dispuesto en el RGPD y la LO 3/2018 y la LO 7/2021 de 26 de mayo, *de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales*, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables (art. 5.2 LO 3/2018 y art. 236 ter 1 y 2 LOPJ).

En consecuencia, dicha Guía Básica se dirigió a las unidades que integran la Fiscalía General del Estado (Unidad de Apoyo, Secretaría Técnica, Inspección Fiscal y Unidades Especializadas), a la Fiscalía del Tribunal Supremo, a la Fiscalía ante el Tribunal Constitucional, a la Fiscalía de la Audiencia Nacional, a las Fiscalías Especiales (Fiscalía Antidroga y Fiscalía contra la Corrupción y la Criminalidad Organizada), a la Fiscalía del Tribunal de Cuentas, a la Fiscalía Jurídico Militar, a las fiscalías de las CCAA, a las fiscalías provinciales y a las fiscalías de área (apartado 7.3 Instrucción FGE 2/2019).

En virtud de todo ello se trasladó la necesidad de observar, entre otras, las siguientes pautas e indicaciones:

1. En relación al acceso a sedes e instalaciones del Ministerio Fiscal, en los casos en que la Institución disponga de edificios o sedes

independientes, la fiscalía, órgano o unidad allí alojada deberá, por un lado, conocer las medidas de seguridad implantadas y, por otro, asumir la responsabilidad respecto del registro de acceso que se lleve a cabo, ya sea por las FFCCSS o por empresas de seguridad privada, sobre personas ajenas al Ministerio Fiscal no siendo preciso el registro de acceso de aquellas personas que habitualmente presten sus servicios en la correspondiente sede del Ministerio Fiscal.

En el caso de que las unidades, órganos o fiscalías se integren en edificios judiciales, se habrá de procurar el establecimiento de medidas de acceso restringido o controlado a la oficina fiscal y a los despachos de los/as fiscales en los que se deposite o pueda depositar documentación, carpetillas, procedimientos y expedientes en soporte papel, así como el cierre de aquellos en ausencia del/los titular/es del despacho y una vez finalizada la jornada laboral.

2. Respecto a la documentación de las actuaciones que se llevan a cabo en materia de protección de datos personales se recordó que la Instrucción FGE 2/2019 dispone que las actuaciones que se realicen para la implementación de la normativa de protección de datos se consignarán en un expediente gubernativo incoado al efecto mediante el correspondiente decreto [apartado 7.3 a)].

De igual modo se señaló que el expediente gubernativo de protección de datos no debe entenderse como un mero repositorio de documentos ya que tiene por objeto la acreditación documental de las actuaciones realizadas por cada fiscalía, órgano o unidad en materia de protección de datos y su existencia se deriva de la primordial obligación que se exige al responsable del tratamiento, en virtud del principio de responsabilidad proactiva (art. 5.2 RGPD), de demostrar que cumple con el resto de los principios relativos al tratamiento de datos (licitud, lealtad, transparencia, limitación de finalidad, minimización, exactitud, limitación de plazo de conservación, integridad y confidencialidad).

En cuanto a los documentos que debe contener el expediente gubernativo de protección de datos, son:

– Decreto de incoación.

– Instrucciones y comunicaciones que emanen de la Fiscalía General del Estado en materia relacionada con la protección de datos personales.

– Registro de Actividades de Tratamiento (RAT).

En relación al RAT se señaló que el RGPD ha sustituido la obligación de dar de alta los ficheros de datos personales por la elaboración de un registro que ha de plasmar el conjunto de actividades de trata-

miento que se realicen, en este caso, por el Ministerio Fiscal y es una de las exigencias que se impone a los responsables para demostrar que el tratamiento que efectúan se lleva a cabo lícitamente y de conformidad con la normativa de protección de datos. Las respectivas actividades de tratamiento agrupan actuaciones y operaciones de distinta naturaleza pero que se realizan con una finalidad u objetivo común.

Dicho registro también tiene por objeto cumplir con el deber de colaboración con la autoridad de control, y se justifica en el caso del Ministerio Fiscal, en el principio de transparencia, lo cual exige que se haga público por medios electrónicos, siendo esta la razón por la que el inventario general de las actividades de tratamiento del Ministerio Fiscal se encuentra publicado en el portal *fiscal.es.*

Sin perjuicio del inventario o registro general de las actividades de tratamiento que realiza el Ministerio Fiscal en su conjunto, es preciso tal como recoge la Instrucción FGE 2/2019, que cada fiscalía, órgano o unidad disponga de un registro propio que refleje las concretas actividades de tratamiento que efectivamente desarrolle.

– Comunicaciones emitidas por el DPD del Ministerio Fiscal las cuales, en su caso, según la naturaleza y contenido de las mismas, deberán ser difundidas a la plantilla de fiscales y funcionarios.

– Instrucciones y notas de servicio emitidas por las respectivas jefaturas a la plantilla de fiscales y funcionarios en materia de protección de datos. Constancia documental de su efectiva difusión.

– Intercambio de comunicaciones entre las respectivas jefaturas con las administraciones prestacionales en materia de protección de datos (p. ej. solicitudes de medios materiales y/o tecnológicos, incidentes de seguridad, comunicaciones de intervenciones en los ordenadores de los fiscales y de la oficina fiscal por parte de la administración prestacional, etc.).

– Comunicaciones relacionadas con esta materia mantenidas con el Delegado de Protección de Datos y sus adjuntos (p. ej. consultas, comunicación de posibles incidentes de seguridad, etc.).

– Modelo de Información de derechos actualizado cuando los datos hayan sido obtenidos de los mismos, cuestión a la que se hace referencia en el apartado 7.3 g) y 7.3 h) de la Instrucción FGE 2/2019.

– Respecto de Fiscalías de CCAA, tratamiento de la materia de protección de datos personales en las Comisiones Mixtas entre el Ministerio Fiscal, Ministerio de Justicia y CCAA con competencia trasferida en materia de justicia.

– Cualquier otra actuación relacionada con la protección de datos personales (p.ej. posibles incidentes de seguridad, actuaciones perió-

dicas desarrolladas con el fin de concienciar a fiscales y funcionarios –fundamentalmente a los de reciente incorporación– acerca de sus obligaciones en materia de protección de datos personales, etc.).

3. Adopción de medidas en seguridad en materia de protección de datos.

La Política de Seguridad de la Información Judicial Electrónica (PSIJE) se aprobó en octubre de 2019 por el Comité Técnico Estatal de la Administración Judicial Electrónica (CTEAJE) en cumplimiento del mandato contenido en el artículo 47.2.b) y en desarrollo del artículo 54 de la 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 cual ha de observarse en los sistemas y aplicaciones que prestan servicio a la Administración de Justicia.

La PSIJE, en su art. 1.3 y 1.4, dispone que afecta a la información, tanto de carácter jurisdiccional como no jurisdiccional, tratada por medios electrónicos, así como a toda la información en soporte no electrónico que haya sido causa o consecuencia directa de la citada información electrónica en la Administración de Justicia siendo de obligado cumplimiento para las fiscalías y todos sus integrantes, y la seguridad de la información afecta a todos los miembros de la organización y a todas las actividades (art. 1.4 y 12.1).

Tal como señala la Instrucción FGE 2/2019, las exigencias que impone la normativa de protección de datos se extienden tanto a quienes integran el MF como a la plantilla de funcionarios que prestan servicio en las distintas fiscalías y órganos fiscales, correspondiendo a los/as fiscales jefes/as dictar instrucciones con el fin de concienciar en la cultura de protección de datos y de instar a su cumplimiento, promover medidas básicas así como difundir las pautas de seguridad que los correspondientes encargados de tratamiento, como proveedores de los medios y aplicaciones informáticas, hayan establecido para su utilización y ello sin perjuicio de las obligaciones que en este sentido a estos también les corresponde.

En consecuencia, para evitar posibles riesgos y brechas que puedan generar incidentes de seguridad, todos están obligados a conocer y cumplir las normas, procedimientos, e instrucciones impartidas en materia de protección de datos para lo cual se habrá de instar a la participación en actividades de formación y concienciación en materia de protección de datos y seguridad de la información.

En virtud de ello, en la referida Guía, se plasmaron más de cuarenta medidas a observar respecto de la seguridad de la documentación e información.