Guía Básica de Actuaciones en materia de Protección de Datos Personales

INDICE

1. Objeto y ámbito de aplicación

El Delegado de Protección de Datos del Ministerio Fiscal (DPD) emite esta Guía Básica en base a las funciones que tiene atribuidas [en el Reglamento (UE) 2016/679 -Reglamento General de Protección de Datos- (RGPD) y demás normativa de aplicación, así como en la Instrucción FGE 2/2019, *sobre la protección de datos en el ámbito del Ministerio Fiscal: el responsable y el Delegado de Protección de Datos*] de informar y asesorar al responsable y a la plantilla de fiscales y de funcionarios que se ocupen del tratamiento de las obligaciones que les incumben en esta materia.

La finalidad de la presente Guía no es la de suplir ni simplificar la normativa vigente, las instrucciones que en esta materia se impartan por la Fiscalía General del Estado o las recomendaciones o pautas dictadas por las administraciones prestacionales (Ministerio de Justicia y Comunidades Autónomas con competencias transferidas) en su ámbito competencial (fundamentalmente, en este caso, en lo que se refiere a la seguridad de la información) a cuyo conocimiento y cumplimiento se encuentran obligados todos los miembros del Ministerio Fiscal y los componentes de la oficina fiscal, sino que tiene por objeto, fundamentalmente, orientar y facilitar la aplicación efectiva de la normativa vigente en el desarrollo de la labor cotidiana de las fiscalías así como concienciar en la cultura de protección de datos.

Esta Guía, al plasmar actuaciones básicas a desarrollar y ejecutar, tiene cierta vocación de perdurabilidad, no obstante será objeto de 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 que se dicten por la Fiscalía General del Estado, de indicaciones que se establezcan por medio de la PSIAJE (Política de Seguridad de la Información de la Administración Judicial Electrónica) o por parte de las administraciones prestacionales así como para, cuando se estime necesario, hacer llegar a todos los integrantes del Ministerio Fiscal pautas encaminadas a mejorar la observancia e implementación práctica de la normativa de protección de datos.

A su vez, la presente Guía tiene por objeto la corrección de deficiencias en la implementación de la normativa de protección de datos, así como reflejar todos aquellos aspectos que podrán ser objeto de verificación y supervisión.

La Instrucción FGE 2/2019, cuyo conocimiento por los miembros del Ministerio Fiscal es fundamental para el correcto entendimiento de esta Guía Básica, 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 se llevan a cabo por medio de las jefaturas de los órganos fiscales, unidades y fiscalías que realizan actividades de tratamiento puesto que su dirección y organización se ejerce en representación del Ministerio Fiscal (arts. 2.1 y 22 EOMF), así como también por medio de los fiscales y funcionarios que forman parte de la plantilla.

En consecuencia, esta Guía se dirige a aquellos órganos, unidades y fiscalías que deben procurar el cumplimiento de esta normativa y concretamente: 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).

No obstante, se ha de tener en cuenta que, dado que esta Guía se dirige al Ministerio Fiscal en su conjunto, alguna de las pautas y orientaciones que contiene solo serán de aplicación, según las circunstancias y actuaciones que efectivamente se realicen, a determinadas fiscalías, órganos o unidades.

2. Difusión

A las respectivas jefaturas corresponderá dar al contenido de esta Guía la difusión debida para su conocimiento y cumplimiento por todos los miembros de las respectivas plantillas, tanto de fiscales como de componentes de la oficina fiscal, debiendo hacerse hincapié en la obligación de observar aquellos deberes a aquellos que directamente conciernan.

3. Actualización

La presente Versión 2.0 de la Guía Básica de Actuaciones en materia de protección de datos actualiza y sustituye a la anterior Versión de Junio de 2022 y a sus anexos.

4. Pautas e indicaciones

4.1. Documentación

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)].

El expediente gubernativo de protección de datos tiene por finalidad acreditar documentalmente las actuaciones que se llevan a cabo por cada fiscalía, órgano o unidad en materia de protección de datos. Por tanto, su tramitación, a diferencia del resto de los expedientes a los que hace mención el art. 9.3 del Reglamento del Ministerio Fiscal, no tiene como objetivo final concluir con una resolución.

La imposición de su tramitación 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 consecuencia, y se ha de insistir en ello, el mismo constituye el medio para acreditar la actividad que el Ministerio Fiscal realiza al objeto de cumplir con la normativa de protección de datos por lo que nunca debe entenderse como un mero repositorio de documentos.

Dicho expediente deberá ser incoado y tramitado en cada fiscalía, órgano o unidad a que se ha hecho referencia en el Apartado 1 de esta Guía.

Las secciones territoriales, aunque obviamente también están obligadas a cumplir con la normativa de protección de datos, no han de incoar y tramitar el referido expediente a fin de documentar todas las actuaciones que se realicen para la implementación de la normativa de protección de datos ya que dicha tarea, en lo que a ellas también respecta, corresponde a la respectiva fiscalía provincial al formar parte de estas (art. 18.2 EOMF)

Por otro lado, la Instrucción FGE 2/2019 también dispone que determinadas actuaciones relacionadas con protección de datos deberán ser tramitadas en expedientes individualizados y separados y ello de conformidad también con lo establecido en el mencionado art. 9.3 del Reglamento del Ministerio Fiscal.

Por tanto, para hacer compatibles ambas exigencias se considera conveniente el establecimiento de alguna referencia que indique la vinculación del contenido de dichos expedientes con la materia de protección de datos, así como, en su caso, la posibilidad de remitir, al expediente de protección de datos, testimonio o copia de aquello que se estime oportuno de cara a cumplir con el referido principio de responsabilidad proactiva.

Documentos que debe contener el expediente gubernativo de protección de datos:

- **Decreto de incoación.**

- **Instrucciones y comunicaciones que emanen de la Fiscalía General del Estado en aquellas cuestiones relacionadas con la protección de datos personales**.

Así, al menos y hasta la presente fecha, debieran figurar:

- Instrucción FGE 2/2019, *sobre la protección de datos en el ámbito del Ministerio Fiscal: el responsable y el Delegado de Protección de Datos.*

- “Buenas prácticas para la gestión de archivos” elaboradas por la Unidad de Apoyo de la FGE.

- Comunicación, de 6 de octubre de 2021, denominada “Implementación de las recomendaciones del DPD en materia de comunicación” emitida por la Secretaría Técnica de la FGE.

- **Registro de actividades de tratamiento** (RAT).

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 tratamiento que se llevan a cabo, 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 deber de transparencia lo cual exige que se haga público por medios electrónicos. Por esta razón 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.

En el registro de cada una de las actividades ha de figurar: el Ministerio Fiscal como responsable de tratamiento especificándose también, en el mismo apartado del responsable, la concreta fiscalía, órgano o unidad y los datos de contacto de la misma; el correo electrónico del Delegado de Protección de Datos (fge.delegadoprotecciondatos@fiscal.es); la finalidad del tratamiento; la categoría de interesados a los que afecta; la categoría de datos personales tratados; los destinatarios a los que se pueden comunicar esos datos; en su caso las transferencia internacional de datos; los plazos previstos, en su caso, para la supresión de los mismos y, cuando sea posible, las medidas de seguridad adoptadas. En el registro de cada una de las actividades de tratamiento también se incluye la base jurídica con el fin de mejor satisfacer las exigencias que se derivan del principio de transparencia.

A dicho inventario se puede acceder por medio del siguiente enlace https://www.fiscal.es/registro-de-actividades-de-tratamiento el cual, a su vez, constituye el modelo a seguir por cada fiscalía, órgano o unidad.

No podrán incorporarse en los registros propios ninguna actividad de tratamiento distinta a las recogidas en dicho inventario sin el previo conocimiento del Delegado de Protección de Datos y la aprobación de la Fiscalía General del Estado.

- **Comunicaciones emitidas por el DPD del Ministerio Fiscal** y por los correspondientes Adjuntos al DPD.

Así, y en virtud de ello, la presente Guía deberá ser incorporada al referido expediente.

- **Instrucciones y notas internas o de servicio emitidas por las respectivas jefaturas y dirigidas a la plantilla de fiscales y funcionarios en materia de protección de datos.**

Las referidas instrucciones o notas de servicio han de tener por objeto, básicamente, difundir y recordar las obligaciones que incumben a todos los fiscales y a los componentes de la oficina fiscal, así como concienciar en la cultura de protección de datos personales comunicando, de este modo, las directrices que se fijen por las correspondientes jefaturas, así como las instrucciones y comunicaciones remitidas por la FGE, la administración prestacional en materia de seguridad y las pautas y recomendaciones emitidas por el Delegado de Protección de Datos siempre que, según su naturaleza y contenido, deban ser difundidas a la plantilla de fiscales y funcionarios.

Se deberá incorporar también la 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 y consultas relacionadas con esta materia mantenidas con el Delegado de Protección de Datos y sus adjuntos.**

- **Actas de las Comisiones Mixtas** entre el Ministerio Fiscal, Ministerio de Justicia y CCAA con competencia trasferida en materia de justicia cuando se aborden cuestiones relativas al tratamiento de datos personales.

- **Cualquier otra actuación relacionada con la protección de datos personales** (p.ej. certificaciones emitidas por las unidades tecnológicas relativas a la irrecuperabilidad de la información contenida en soportes electrónicos de información, testimonio de expedientes incoados por posibles incidentes de seguridad, actuaciones periódicas 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.).

- **Modelo de Información de derechos a los interesados**.

4.2. Información de derechos a los interesados

A la cuestión relativa a la información de derechos a los interesados, cuando los datos hayan sido obtenidos de los mismos se hace referencia en el apartado 7.3 g) de la Instrucción FGE 2/2019.

La información de derechos responde al principio de transparencia y al deber de información que corresponde al responsable (arts. 12 y 13 RGPD, art. 11 LO 3/2018 y art. 21 LO 7/2021) así como a la exigencia plasmada en la Instrucción FGE 2/2019, en el sentido de que cuando los datos personales hayan sido obtenidos del propio interesado a raíz de la presentación de un escrito, denuncia o queja, se le deberá facilitar una información concisa, transparente, inteligible y de fácil acceso relativa al tratamiento de sus datos personales.

Por tanto, en la primera interacción que se mantenga con los interesados (toda persona física identificada o identificable), y únicamente en ese primer contacto, se les deberá proporcionar la información de derechos de protección de datos.

Dicha información de derechos también debiera suministrarse a los fiscales cuando se produzca su efectiva incorporación a la carrera fiscal, así como a los funcionarios cuando sean destinados, por primera vez, a cualquier oficina fiscal.

Para cumplir con la referida obligación, la información se ha de suministrar por niveles o capas. Es decir, en lo que sería la primera capa se ha de incluir un nivel básico de la información requerida, de forma estructurada y muy concentrada, la cual ha de remitir, a su vez, a un segundo nivel el cual deberá contener una información más detallada.

El objetivo de este sistema es conciliar el deber de informar con la exigencia de que esa información se transmita de forma concisa, inteligible y con un lenguaje claro y sencillo.

La tarea de aunar ambas obligaciones no resulta sencilla, puesto que cumplir la primera (informar de forma concisa) sin tener en cuenta la segunda (informar de forma clara y sencilla) debilitaría el derecho de los interesados a recibir una información adecuada y comprensible recogido en el RGPD y podría llegar a considerarse una infracción de sus disposiciones.

Por ese motivo, el modo más correcto para cumplir con el deber de transparencia es informar de modo directo al interesado mediante un sencillo impreso de información de derechos (primera capa) en el que se contenga un enlace a la dirección web https://www.fiscal.es/ejercicio-de-los-derechos donde se recoge información más desarrollada (segunda capa).

El modelo a utilizar será el que figura en el Anexo I.

Cuando la denuncia, escrito o queja se presente mediante un formulario web o se reciba por correo electrónico, se deberá, respectivamente, habilitar el acceso al modelo de información de derechos mediante el correspondiente enlace al sitio web donde este se encuentre o remitir la referida información junto con el correspondiente acuse de recibo.

4.3. Ejercicio de los derechos por los interesados

El art. 236.1 septies LOPJ, en relación con el tratamiento de datos con fines jurisdiccionales, dispone que los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados. Estos derechos deberán ejercitarse ante las fiscalías en las que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

A su vez, el apartado 3 de ese mismo artículo establece, en relación con el tratamiento de los datos personales con fines no jurisdiccionales, que los interesados podrán ejercitar los derechos de información, acceso, rectificación, supresión, oposición y limitación en los términos establecidos en la normativa general de protección de datos.

En relación con la solicitud de ejercicio de derechos resulta fundamental tener en cuenta el apartado 7.3 h) de la Instrucción FGE 2/2019, así como, en lo que respecta a las diligencias de investigación, el apartado 17 de la Circular 2/2022, de 20 de diciembre, *sobre la actividad extraprocesal del Ministerio Fiscal en el ámbito de la investigación penal*.

El ejercicio de los derechos deberá ejercitarse ante las fiscalías, órganos o unidades en las que se tramite el procedimiento para lo cual los interesados, tal y como figura en el modelo de impreso que se acompaña en el Anexo I, podrán dirigirse a la fiscalía, unidad u órgano fiscal a través del formulario que se contiene en la dirección web: https://www.fiscal.es/ejercicio-de-los-derechos.

4.4. Reclamaciones efectuadas por los interesados

Tal como figura en el modelo de impreso de información de derechos que se contiene en el Anexo I (también en el Anexo II al cual se hace referencia en el apartado 4.11), el interesado debe ser informado de que caso de considerar que se han visto afectados sus derechos o de no darse curso a su solicitud de ejercicio de los mismos podrá, antes de formular reclamación ante la Agencia Española de Protección de Datos, dirigirse al Delegado de Protección de Datos del Ministerio Fiscal por medio de la dirección de correo electrónico: fge.delegadoprotecciondatos@fiscal.es .

Se ha de tener en cuenta que cuando entre en funcionamiento la Unidad de Protección de Datos del Ministerio Fiscal, contemplada en la reforma del EOMF operada por Ley Orgánica 1/2025, de 2 de enero, *de medidas en materia de eficiencia del Servicio Público de Justicia*, y exclusivamente respecto al tratamiento de datos con finalidad jurisdiccional, no cabrá esa posibilidad ya que las funciones que ahora se le atribuyen al DPD en el art. 22.2 del Reglamento del Ministerio Fiscal y en el apartado 8.2.1 de la Instrucción FGE 2/2019 quedaran implícitamente derogadas ya que ambos órganos quedan refundidos en uno al no ser precisa, en ese ámbito de tratamiento, la existencia de un Delegado de Protección de Datos (art. 40.1 LO 7/2021). En este caso,

los reclamantes deberán dirigirse directamente a la Unidad de Protección de Datos la cual, por otro lado y a su vez, asume la condición de DPD en lo que al tratamiento de datos no jurisdiccionales se refiere.

Para dar curso o tramitar las reclamaciones efectuadas por los interesados (por falta de atención de una solicitud de ejercicio de los derechos o por la posible infracción de la normativa de protección de datos) las fiscalías, órganos o unidades objeto de aquellas deberán proceder a la apertura de los correspondientes expedientes gubernativos [apartado 7.3 a) *in fine* de la Instrucción FGE 2/2019 y 9.3 del Reglamento del Ministerio Fiscal].

4.5. Implementación del principio de minimización

Por datos personales se ha de entender toda información sobre una persona física identificada o identificable (el interesado). Se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos 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 [art. 4.1 RGPD y art. 5 a) LO 7/2021].

La LOPJ dispone, respecto del principio de minimización, que las resoluciones y actuaciones procesales del Ministerio Fiscal solo deberán contener aquellos datos que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, en especial para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso pueda producirse indefensión (art. 236 quinquies 1 y 2).

En virtud de ello:

- En la tramitación de las diligencias de investigación, diligencias preprocesales y expedientes gubernativos se procurará evitar el traslado de copia íntegra de lo actuado cuando contengan datos personales que no precisen ser conocidos por el resto de las partes o por otros intervinientes en las mismas. Con esa finalidad se deberán adoptar las medidas necesarias para la supresión de los datos personales de las resoluciones y de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar el derecho a tutela judicial efectiva o indispensables para los fines de las propias diligencias o expedientes.

Por tanto, en cada caso y con el mayor rigor, deberá examinarse la pertinencia de dar a conocer al resto de los intervinientes en diligencias de investigación, diligencias preprocesales y expedientes, datos personales o determinados datos personales de las otras partes mereciendo singular cautela la comunicación de datos especialmente protegidos (por ej. datos relativos a la salud) procediendo a la eliminación o seudonimización de aquellos que no sean imprescindibles (domicilio, documento de identidad, teléfono, etc.).

- De igual modo, en el contenido de los decretos que se dicten en diligencias de investigación, diligencias preprocesales y expedientes gubernativos se habrá de procurar limitar, en la medida de lo posible, la consignación de aquellos datos personales que no sean precisos para pronunciarse o resolver sobre la cuestión planteada.

- La limitación de consignación de datos personales que no sean precisos para pronunciarse o resolver sobre la cuestión planteada se aplicará también a cualquier escrito o dictamen realizado por el Ministerio Fiscal.

Así, en los escritos de calificación respecto de la identificación de los acusados pudiera ser suficiente a efectos de su identificación (obviamente además del nombre y apellidos) de únicamente cuatro cifras numéricas aleatorias del correspondiente documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente, y ello en términos semejantes a lo dispuesto en la Disposición Adicional Séptima 1 de la LO 3/2018.

La limitación de la consignación de cifras numéricas pudiera hacerse extensiva, siempre según las concretas circunstancias del caso, a otros datos personales identificativos (de cualquier parte o interviniente en el proceso) de carácter numérico o alfanumérico que se pudieran consignar en los dictámenes del Ministerio Fiscal tales como números de cuentas corrientes u otros datos bancarios de naturaleza similar, números de teléfonos, IMEIs, IPs, datos catastrales, matriculas de vehículos, etc.

Semejantes consideraciones, respecto de la implementación del principio de minimización, cabría hacer respecto a fechas de nacimiento y a direcciones de correo electrónico o postal.

En lo que se refiere a la proposición de prueba testifical y pericial y la localización de los mismos para su posterior citación, en base al artículo 656 LECrim., debería bastar la consignación del folio del procedimiento en soporte papel en que figure el mismo y, en caso de expediente digital, la del número de acontecimiento y, dentro del mismo, su concreto folio.

La razón de todo ello se encuentra en que la aplicación de la norma procesal por parte de todos los operadores jurídicos se ha de interpretar a la luz de la normativa de protección de datos y ha de observar las exigencias impuestas por los principios que constituyen el fundamento de este derecho fundamental. Ello supone que las resoluciones y actuaciones procesales que se lleven a cabo deberán cumplir, entre otros, con el mencionado principio de minimización [art. 6 LO 7/2021 y 236 quinquies 1) LOPJ].

Las anteriores pautas han de aplicarse de manera razonable y ponderada, teniendo siempre presente que el derecho de los interesados a la protección de datos no puede prevalecer sobre el derecho a la tutela judicial efectiva ni impedir el ejercicio de las funciones que el Ministerio Fiscal tiene encomendadas y que la aplicación del principio de minimización de datos no puede exacerbarse de tal modo que llegue a convertir en crípticas o incomprensibles las resoluciones que se dicten.

4.6. Limitación del plazo de conservación

El Convenio 108 modernizado del Consejo de Europa de 2018 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal dispone, en su art. 5.4.e), que los datos personales deberán preservarse de forma tal que permitan identificar a los titulares de datos, por no más tiempo que el necesario para los propósitos en función de los cuales se tratan dichos datos.

A su vez, el art. 5.1 e) RGPD consagra el principio de limitación del plazo de conservación al disponer que los datos personales serán "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado".

Por otro lado, el RPGP, en virtud del principio de protección de datos desde el diseño y por defecto, exige al responsable del tratamiento aplicar "las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad" (art. 25.2).

De igual modo, la Instrucción FGE 2/2019, en su apartado 7.1, señala que el MF estará obligado a tratar los datos personales de las personas físicas de acuerdo con los principios relativos al tratamiento siendo uno de ellos el de limitación del plazo de conservación, lo que supone que, en el marco de sus competencias y en la medida de lo posible, deberá adoptar medidas razonables para que los datos personales sean mantenidos de forma que se permita la identificación de los interesados durante el tiempo estrictamente necesario para los fines del tratamiento.

En sentido similar, en lo que se refiere a la protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, atendiendo a lo dispuesto en el art. 8 de la Ley Orgánica 7/2021, corresponderá al Ministerio Fiscal:

1. Determinar que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los mencionados fines.

2. Revisar la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad, como máximo cada tres años, atendiendo especialmente en cada revisión a la edad del afectado, el carácter de los datos y a la conclusión de una

investigación o procedimiento penal. Si es posible, se hará mediante el tratamiento automatizado apropiado.

También, según dispone dicho artículo, con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurran factores como la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesario el tratamiento de los datos para el cumplimiento de los mencionados fines.

En virtud de todo ello el Ministerio Fiscal como responsable del tratamiento está obligado, salvo que exista una exigencia legal u obligaciones de inspección o supervisión interna que a esos efectos requieran la conservación temporalmente limitada de determinados documentos, a suprimir sin dilación indebida los datos personales cuando ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo (art. 17.1 RGPD).

No obstante, y sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la normativa de protección de datos, podrán ser conservados aquellos documentos del Ministerio Fiscal que contengan datos personales, tanto en soporte papel como digital, que, por su relevancia histórica, social o económica, o como puntuales ejemplos que sirvan de testimonio histórico de un determinado modo de hacer, pasen a formar parte del patrimonio documental de conformidad con el art. 49.2 de la Ley 16/1985, de 25 de junio, *del Patrimonio Histórico Español*. Los criterios al respecto deberán ser definidos por la Fiscalía General del Estado o en su defecto, y hasta en tanto ello se lleve a cabo, por las correspondientes jefaturas.

4.7. Deber de confidencialidad por parte de terceros

En el artículo 236 quinquies 3 LOPJ se dispone que los datos personales que las partes conozcan a través del proceso deberán ser tratados por estas de conformidad con la normativa general de protección de datos. Esta obligación también incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

A fin de recordar a los destinatarios el obligado cumplimiento del deber de confidencialidad, en los correspondientes oficios de notificación y/o remisión de las resoluciones y escritos del Ministerio Fiscal, se habrá de incluir como pie de página la siguiente cláusula:

La comunicación de los datos de carácter personal que pudieran figurar en el documento adjunto, no previamente seudonimizados o anonimizados, se realiza en cumplimiento de las funciones legales y estatutarias encomendadas al Ministerio Fiscal y al amparo de la vigente normativa de protección de datos.

La referida normativa también es de aplicación al destinatario o destinatarios de esos datos personales los cuales no podrán ser objeto de tratamiento ulterior con una finalidad distinta a la que ha motivado su actual comunicación. En todo caso deberán adoptarse las medidas necesarias para evitar cualquier tratamiento no autorizado o ilícito.

Por otro lado, tras los pies de firma de los correos electrónicos corporativos de forma automatizada normalmente se incluye un requerimiento de confidencialidad dirigido a aquellos que por error pudieran recibir el correo electrónico que se envía.

De no figurar por defecto en la aplicación de correo facilitada por la administración prestacional la referida información, resulta aconsejable la inclusión de una advertencia como la siguiente:

Este mensaje ha sido enviado a la dirección del destinatario. Puede contener información privilegiada, cuya divulgación esté protegida y/o de carácter confidencial. Está prohibido realizar cualquier reseña, difusión o uso de la información contenida en este documento por persona distinta a la del destinatario. Si usted ha recibido esta transmisión por error, por favor, tenga la amabilidad de notificarlo al remitente y destruya esta transmisión.

This message has been sent to the address of the addressee. It may contain privileged and/or confidential information, which is protected from disclosure. It is forbidden to make any review, diffusion or use of the information contained in this document by anyone other than the addressee. If you have received this message by mistake, please kindly notify the sender and destroy it.

Sin perjuicio de ello, se habrá de procurar evitar dicho error mediante una comprobación consciente de la dirección o direcciones de correo antes de proceder al envío.

4.8. Relación con los medios de comunicación

Respecto de esta cuestión se habrá de tener en cuenta la Comunicación difundida por la Secretaría Técnica de la Fiscalia General del Estado el 6 de octubre de 2021 denominada "*Implementación de las Recomendaciones del DPD del Ministerio Fiscal en materia de comunicación*".

La Instrucción FGE 3/2005, *sobre las relaciones del Ministerio Fiscal con los medios de comunicación*, insta a que por el Ministerio Fiscal se asuma un rol activo en el desarrollo de esa facultad que viene atribuida estatutariamente, por lo que debe tomar

la iniciativa e informar en todos los casos de relevancia social desde el momento de la iniciación del proceso dado que cuando concurre interés informativo sobre un determinado proceso, los medios acaban por suministrar la información requerida, aunque sea a espaldas de las instancias oficiales.

Tal como señala la mencionada Instrucción FGE 3/2005, el cumplimiento de esa facultad-deber de información ha de acomodarse a los principios que en general estructuran el Ministerio Público. Funcionalmente, la actuación en el ámbito informativo conforme a la imparcialidad y la legalidad asegurará la corrección de los contenidos transmitidos a los medios. Orgánicamente, la estructuración conforme a los principios de unidad de actuación y de dependencia jerárquica facilitará la coherencia y la eficacia en la política informativa de la Fiscalía.

A su vez, se ha de tener en cuenta que, según la Instrucción FGE 2/2019, *sobre la protección de datos en el ámbito del Ministerio Fiscal*, este es responsable del tratamiento de datos personales y en consecuencia se encuentra obligado, al igual que otros poderes públicos, a tratar los datos personales de las personas físicas de acuerdo con las disposiciones y principios que rigen esta materia, entre los que se encuentra el principio de minimización, contemplado en el art. 5.1 c) del RGPD, el cual dispone que los datos han de ser tratados de modo adecuado, pertinente y limitado a lo necesario en relación con los fines para los que son tratados.

Entre las reservas y garantías exigibles a la hora de comunicar información a los medios, se encuentra el deber de velar por los derechos de los afectados (en base a los art. 124 CE, 1 y 3.3 EOMF), teniendo especial significación, el derecho fundamental a la protección de datos personales, ya que el mismo entra en juego siempre que se traten datos de esta naturaleza siendo, pese a su estrecha conexión, un derecho diferenciado y de distinta significación al de la intimidad.

Lo anterior conlleva necesariamente el previo examen y ponderación de los mencionados intereses en juego (en lo que aquí se trata, deber de información y deber de protección de datos personales) sopesando, en cada caso, si resulta preciso o no, para satisfacer esa facultad/deber de información a los medios, comunicar datos personales de cualquiera de las personas físicas que de un modo u otro tienen intervención en los correspondientes procesos, diligencias o expedientes.

Conciliar la facultad/deber de información con el derecho a la protección de datos personales es una labor que habrá de realizarse caso por caso con el fin de lograr el justo equilibrio entre ambos ya que, dada la ilimitada casuística que se puede generar, no es posible establecer unas pautas generales para resolver dicha cuestión.

No obstante, como criterios orientativos, en línea con lo marcado en este aspecto por la Instrucción FGE 3/2005 se habrá de evitar la transmisión de datos personales en aquellos supuestos en los que la comunicación de los mismos pueda comprometer derechos fundamentales del interesado o de terceros (por ej. seguridad, defensa, tutela judicial efectiva, intimidad, honor, propia imagen de las víctimas); generar un innecesario daño reputacional o incluso cuando esos datos personales no aporten valor añadido alguno o dato noticiable adicional relevante al acontecimiento que se comunica.

De igual modo, aunque la doctrina del Tribunal Europeo de Derechos Humanos no considera infringido el deber de reserva cuando el objeto de la revelación ya es conocido por todos, al no ser secreto lo que ya es de dominio público, ello no significa que habiendo sido difundidos previamente datos personales de una persona física, el Ministerio Fiscal en posteriores o sucesivos comunicados haya de hacer explicita referencia a los mismos dado que, en base al principio de minimización en tratamiento de datos, deberá limitar, en la medida de lo posible, el efecto multiplicador que ello puede suponer, razón por la que deberá valorar las circunstancias del caso y los diversos intereses involucrados a la hora de determinar la extensión de la información a suministrar.

Por otro lado, los medios de comunicación, sin perjuicio de las excepciones que se puedan contemplar, no están exentos de cumplir la normativa de protección de datos, pudiendo los distintos medios, respecto de un hecho noticiable, en el ejercicio de su libertad profesional, acudir a otras fuentes y decidir la forma y los contenidos de la información a transmitir, teniendo en cuenta que estos, en el ejercicio de tan trascendental tarea podrán adoptar posturas distintas en relación a los datos que aportan respecto de los posibles afectados.

Así, la LO 3/2018, además de contemplar en el art. 85 el derecho de rectificación en internet recoge, en el art. 86, el derecho de toda persona a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización respecto de las noticias que le conciernan, pudiendo así ejercer sus derechos aquellos interesados que se consideren perjudicados.

En consecuencia, en los envíos de documentación o información a los medios de comunicación se habrá de incluir una advertencia sobre la responsabilidad de estos respecto de la divulgación de los datos personales contenidos en los mismos, la cual tendrá el siguiente contenido:

Esta comunicación no puede ser considerada como la publicación oficial de un documento público.

La comunicación de los datos de carácter personal que puedan figurar en el documento adjunto, no previamente seudonimizados o anonimizados, se realiza en cumplimiento de la función institucional que el artículo 4.5 de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, a los exclusivos efectos de su eventual tratamiento con fines periodísticos en los términos previstos por el artículo 85 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.

Lo dispuesto en la normativa de protección de datos de carácter personal será de aplicación al tratamiento que los destinatarios de esta información lleven a cabo de los datos personales contenidos en el documento adjunto los cuales, en ningún caso, podrán ser comunicados o difundidos con fines contrarios a las leyes.

4.9. Programas automáticos de seudonimización

El proceso de anonimización permite que la información no pueda asociarse de modo definitivo e irreversible a una persona concreta, identificada o identificable, a diferencia de ello, el proceso de seudonimización supone que los datos no puedan atribuirse a un interesado sin utilizar información adicional.

Esta cuestión tiene su relevancia ya que los datos anonimizados, a diferencia de aquellos seudonimizados, quedan fuera del ámbito de aplicación de la normativa de protección de datos.

El término disociación, aunque se utiliza en el art. 235 de la LOPJ como sinónimo de seudonimización y en contraposición al de anonimización no resulta del todo correcto, ya que en realidad vendría a ser un sinónimo de "anonimización" tal como sostiene la AEPD en diversas resoluciones y en su *Guía de orientaciones y garantías en los procedimientos de anonimización*, cuando define este proceso como la disociación definitiva e irreversible de los datos personales.

Dada la naturaleza de la actividad que desarrolla el Ministerio Fiscal, el proceso que generalmente se seguirá será el de seudonimización ya que, dada la vinculación de los datos personales con procesos, diligencias o expedientes, no será posible garantizar de modo absoluto una anonimización definitiva e irreversible.

Cuando se lleve a cabo el proceso de seudonimización, ya sea de forma manual o automatizada, se habrá de procurar dificultar, en la medida de lo posible la reversibilidad en la identificación de la persona o personas afectadas (p.ej. suprimiendo también aquellos datos o información que permitan identificar al interesado de modo indirecto).

Por tanto, la utilización de programas informáticos que permitan de manera automática la supresión o seudonimización de los datos personales de las partes y otros intervinientes recogidos en los documentos y escritos de los fiscales exigirá también la supervisión personal del resultado de dicho proceso con el fin de evitar que por medio de información relacionada se pueda producir una reidentificación o identificación indirecta de las personas cuyos datos personales se pretenden proteger.

El empleo de esas herramientas tampoco podrá eximir a los miembros del Ministerio Fiscal de realizar, en cada caso, el pertinente juicio de ponderación respecto de otros derechos e intereses que, junto al derecho a la protección de datos, pudieran entrar en juego (p. ej. defensa, tutela judicial efectiva, deber de informar a la opinión pública, etc.)

4.10. Actuaciones en virtud de convenios de cooperación formativa o de investigación

El tratamiento de los datos personales está sometido, entre otros principios, a los de licitud y confidencialidad.

El tratamiento será licito, entre otros supuestos, cuando se realice para el cumplimiento de una misión realizada en interés público, en cuyo caso debe tener una base en el Derecho, la cual se encuentra, en este caso, en la Ley Orgánica 2/2023, del Sistema Universitario y en su normativa de desarrollo.

Por otro lado, los datos personales habrán de ser tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito.

Para ello, en los convenios de cooperación educativa o de investigación con universidades con carácter general y salvo que concurran circunstancias especiales, se considera precisa la inclusión de la siguiente cláusula:

> ***Protección de datos.*** *El tratamiento de los datos personales que se efectué como consecuencia del presente Convenio se llevara a cabo de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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 y por el que se deroga la Directiva 95/46/CE y con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*
>
> *Las partes firmantes se comprometen a adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos personales tratados. A tal fin, por parte del Ministerio Fiscal, únicamente se facilitará a las/los estudiantes/investigadoras/es el acceso a aquellos datos que sean precisos para el desarrollo de las prácticas universitarias/trabajos de investigación.*
>
> *Las/los estudiantes/investigador/as/es estarán obligados a mantener el deber de secreto y confidencialidad respecto de los datos personales que pudieran conocer como consecuencia de las prácticas externas/trabajos de investigación realizados durante su estancia en las fiscalías, incluso una vez que éstas hayan finalizado. Para lo cual deberán suscribir, individualmente, el correspondiente compromiso de confidencialidad.*
>
> *El incumplimiento del deber de secreto y confidencialidad podrá conllevar responsabilidades de naturaleza penal y/o derivadas de la normativa de la protección de datos.*
>
> *Los/as titulares de los datos personales podrán ejercer los derechos previstos en la legislación aplicable ante las entidades firmantes en las direcciones correspondientes.*
>
> *En el caso de la Fiscalía, a través de la dirección web del Ministerio Fiscal* https://www.fiscal.es/ejercicio-de-los-derechos

A su vez, los correspondientes convenios deberán ir acompañados de un anexo que contenga el compromiso de confidencialidad al que se hace referencia en la antes mencionada cláusula (y que individualmente habrán de firmar los estudiantes que participen en la actividad educativa) que habrá de estar redactado en los siguientes términos:

El/la estudiante/investigador/a D./Dª……, con DNI nº….., está obligado/a, y por ello se compromete, a mantener el deber de secreto y confidencialidad respecto de los datos personales que conozca como consecuencia de las prácticas externas realizadas durante su estancia en la Fiscalía, incluso una vez que estas hayan finalizado.

El incumplimiento del deber de secreto y confidencialidad puede conllevar responsabilidades de naturaleza penal y/o derivadas de la normativa de protección de datos.

Por la Jefatura de la correspondiente Fiscalía se habrá de recordar a los fiscales que ejerzan de tutores o responsables de la formación o de la supervisión de la actuación investigadora que únicamente deberán facilitar a los estudiantes/investigadores el acceso a aquellos datos que sean precisos para el desarrollo de las prácticas universitarias o trabajos de investigación, así como la conveniencia de que recuerden a los estudiantes/investigadores su compromiso de confidencialidad.

4.11. Acceso a sedes e instalaciones del Ministerio Fiscal

En los supuestos en los que el Ministerio Fiscal disponga de edificios o sedes independientes 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, así respecto de:

- Seguridad y videovigilancia: Se habrá de conocer la identidad del correspondiente responsable o encargado de tratamiento en materia de seguridad y videovigilancia. Toma de conocimiento de las medidas implantadas.

- Identificación de terceros ajenos a la Fiscalía: Se realizará mediante el establecimiento de control de acceso a las sedes o instalaciones propias del Ministerio Fiscal. No será preciso el registro de acceso de aquellas personas que habitualmente presten sus servicios en la correspondiente sede.

- Aplicación Informatica específica para el registro. Hasta que se cuente con ella dicho registro se podrá llevar a cabo mediante una hoja de Excel, debiendo tenerse en cuenta que al ordenador que la contenga se habrá de acceder mediante un nombre de usuario y una clave personal de uso individual y ello sin perjuicio de cualesquiera otras medidas de seguridad que se estime oportuno implantar.

- Plazo de conservación de los datos personales: Será de un mes desde su recogida por lo que se habrán de establecer pautas de actuación internas con el fin de hacer efectiva dicha limitación de tratamiento.

- Datos personales a recabar: fecha, hora de entrada y salida, nombre y apellidos; número de carnet identidad, NIE o pasaporte; número de teléfono y/o correo electrónico; en su caso, organismo/empresa al que pertenece; fiscal o funcionario al que se visita o motivo del acceso y número de tarjeta identificativa que se asigna.

- Colocación en lugar visible de la información de derechos del registro de acceso en caso de sedes propias del Ministerio Fiscal.

El modelo de impreso de información figura en el Anexo II

En el caso de que las unidades, órganos o fiscalías se integren en edificios judiciales, se procurará el establecimiento de medidas de acceso restringido o controlado a la oficina fiscal y a los despachos de los 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 titular/es del despacho y una vez finalizada la jornada laboral.

4.12. Adopción de medidas en seguridad

En cumplimiento del mandato contenido en el artículo 93 del 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*, el Comité Técnico Estatal de la Administración Judicial Electrónica aprobó, el 21 de junio de 2024, la vigente Política de Seguridad de la Información de la Administración Judicial Electrónica (PSIAJE).

La PSIJAE, en su art. 1.3 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.

El art. 1.4 establece que la PSIAJE será de obligado cumplimiento en el desarrollo de la actividad de los órganos y oficinas judiciales, y de las fiscalías por parte de todos sus integrantes.

A su vez, en el art. 11.2 se dispone que el Ministerio de Justicia y las Administraciones con competencias transferidas en la dotación de medios materiales velarán por el mantenimiento de un nivel óptimo de seguridad en la gestión de los sistemas de información e infraestructuras tecnológicas puestos al servicio de la Administración de Justicia, en calidad de responsables o encargados del tratamiento, así como para la Fiscalía General del Estado, a través de su Comisión Nacional de informática y comunicaciones electrónicas.

De igual modo, la LOPJ dispone que la administración competente deberá cumplir con las responsabilidades que en materia de tratamiento y protección de datos personales se le atribuya como administración prestacional (art. 236 sexies).

La PSIAJE es 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).

En todo caso, la Unidad de Protección de Datos, en ejercicio de las competencias que corresponden a la autoridad de protección de datos con fines jurisdiccionales sobre el tratamiento de los mismos realizados respectivamente por el Ministerio Fiscal u oficinas fiscales, también ostenta la facultad de dictar las instrucciones que estime necesarias en el ejercicio de sus funciones y poderes atribuidos por la LOPJ, el RGPD, LOPDGDD y Ley Orgánica 7/2021, en aquellos supuestos que sean de aplicación (art. 11.3 PSIAJE).

Por otro lado, 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 fiscales jefes 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.

4.12.1. Medidas a observar respecto de la seguridad de la documentación e información.

Por parte de las jefaturas, y sin perjuicio de aquellas otras que se estimen oportunas:

- Reclamar de las administraciones prestacionales la remisión y difusión de las pautas de seguridad que las mismas, como proveedoras de los medios y aplicaciones informáticas, hayan establecido para su utilización.
- Conocimiento y valoración de los acuerdos de confidencialidad por parte del personal de seguridad, mantenimiento y limpieza que preste sus servicios en la respectiva fiscalía.
- Tomar medidas para la destrucción de forma segura de documentos en soporte papel para lo cual se emplearán máquinas trituradoras que se habrán de recabar de la administración prestacional en número suficiente.
  El uso de contenedores de papel abiertos destinados a la destrucción de documentos en los que figuran datos personales debiera descartarse. Por tanto, de utilizarse, debieran ser cerrados y existir el correspondiente acuerdo de confidencialidad con la empresa o entidad gestora cuyos términos deben ser conocidos por la jefatura.
- Supervisar que todos los soportes de información devueltos por sus usuarios, tanto los que vayan a ser reutilizados o a causar baja, sean previamente tratados por la respectiva unidad tecnológica para eliminar permanentemente la

información que pudieran contener, de manera que resulte imposible su recuperación. Las referidas unidades deberán emitir el correspondiente certificado que acredite la irrecuperabilidad de la información.

- Transferencia periódica de documentos desde el archivo de gestión de fiscalía al archivo general o central de aquellos documentos vinculados con procedimientos que no se encuentren en tramitación.
- Recordar el deber de confidencialidad respecto de la información conocida con ocasión del ejercicio de la función, así como de la debida custodia de documentos, carpetillas, procedimientos y expedientes.
- Recordar el deber de custodia de los soportes de información, de llaves y tarjetas de acceso restringido, así como de las tarjetas criptográficas.
- Recordar que el acceso a los sistemas de información únicamente se ha de llevar a cabo con la finalidad exclusiva de que cada usuario pueda cumplir con las funciones atribuidas. Únicamente se podrá acceder y hacer uso de las bases de datos, áreas, carpetas y aplicaciones para las que se esté legitimado o autorizado no debiéndose acceder en ningún caso a información perteneciente a otros usuarios o grupos de usuarios para los que no se posea tal autorización.
- Implantación de mecanismos de identificación, autenticación y autorización de usuarios para el acceso a los activos de información. El referido sistema deberá permitir el registro del acceso físico o la utilización del sistema con objeto de asegurar su trazabilidad y así poder auditar su adecuado uso.
- Establecer que los datos personales de los intervinientes en los procesos, diligencias o expedientes se incluyen en el reverso de la caratula de las carpetillas que contienen documentación en soporte papel.
- Implantación de actuaciones y adopción de medidas dirigidas a impedir que queden a la vista o a disposición de personal no autorizado documentos que contengan datos personales.
- Recordar el deber de depósito y custodia en armarios con cerradura de la documentación, carpetillas, procedimientos y expedientes en soporte papel.
- Implantación de medidas adicionales de protección respecto de asuntos de mayor o especial interés público derivado de las personas de los investigados o la propia naturaleza de los asuntos (por ej. depósito del procedimiento en caja fuerte o armario cerrado específico para el asunto en cuestión, consulta y acceso al procedimiento exclusivamente en dependencias de fiscalía).
- Supervisar que el acceso a carpetas compartidas en la "*nube*" únicamente se lleve a cabo por usuarios autorizados. Para ello puede resultar conveniente la designación de una persona encargada de la actualización de las habilitaciones de acceso a las carpetas compartidas y de la supervisión de su contenido de modo que no se conserven datos personales más allá del tiempo imprescindible para las tareas que se llevan a cabo, promoviendo periódicamente la supresión de toda aquella información y documentación innecesaria.
- Obligación de la jefatura de notificar sin dilación cualquier incidente que pueda suponer la destrucción, pérdida o alteración accidental o ilícita de los datos personales o la comunicación o acceso no autorizado a dichos datos. La plantilla ha de notificarlo a la jefatura y esta al DPD del MF y a la Unidad de Apoyo de la Fiscalía General del Estado. A estos efectos ver el apartado 4.13 de esta Guía.

Por parte de la plantilla de fiscales y funcionarios.

- Cumplir las pautas de seguridad antes mencionadas que les sean de aplicación.
- Puestos de trabajo despejados. Al finalizar la jornada de trabajo, toda la información permanecerá en los armarios, cajones y despachos que garanticen la seguridad de éstos fuera del horario laboral.
- Se tendrá especial cuidado en no dejar anotaciones con credenciales corporativas y/o contraseñas, así como tarjetas criptográficas que puedan ocasionar que personas no autorizadas accedan a información.
- Vigilancia permanente, fuera de entornos seguros, de todos aquellos soportes (papel, dispositivos o equipos informáticos) que contengan datos personales con el fin de evitar extravíos o hurtos que comprometan la información almacenada.
- Utilización en los equipos informáticos de usuario y contraseña de uso personal y no compartido.
- Bloqueo o cierre de sesión en el equipo informático antes de abandonar el puesto de trabajo.
- Comprobación de la retirada de las tarjetas criptográficas del equipo cuanto el usuario no esté haciendo uso del mismo.
- El almacenamiento de información que contenga datos personales en soportes electrónicos portátiles (discos duros externos, memorias USB, etc.) ha de limitarse al máximo siendo obligada su encriptación en caso de que se utilicen.
- Evitar el uso de cuentas privadas de correo electrónico no seguras para comunicaciones que contengan información y/o datos personales cuyo tratamiento sea consecuencia del ejercicio de la función pública atribuida al Ministerio Fiscal.
- Evitar el uso del correo electrónico corporativo para actividades personales de naturaleza reservada. El uso para actividades personales no reservadas deberá restringirse al máximo.
- Utilizar la casilla CCO (copia oculta) con el fin de garantizar el anonimato de los mismos para el resto de los receptores cuando así sea preciso, atendiendo a la condición de los distintos destinatarios.
- En la medida de lo posible, en lugar de compartir documentos por correo electrónico, adjuntar un enlace al contenedor (carpeta de red, Alfresco, etc.).
- No compartir documentos en carpetas a las que puedan tener acceso usuarios que no estén habilitados o no deban conocer su contenido.
- No abrir ni compartir archivos o enlaces adjuntos que puedan acompañar a correos electrónicos remitidos por fuentes desconocidas.
- No almacenar indefinidamente información o documentos en los que figuren datos personales en los soportes digitales ni en las cuentas de correo electrónico. Eliminar los mismos una vez dejen de ser necesarios, asegurándose de que no queden residentes en la papelera.
- Conveniencia de cifrar la información a intercambiar si esta es especialmente sensible. Para ello se puede utilizar la herramienta *7zip* u otras semejantes debiendo compartirse la contraseña con el/los destinatarios por un canal diferente. La condición de datos o información sensible habrá de ser valorada en cada caso atendiendo a criterios tales como la relevancia o trascendencia pública del asunto, volumen de datos personales e información transmitida, etc.

- Cerciorarse de recoger los documentos (fundamentalmente de los originales) de la fotocopiadora, impresora, escáner o fax una vez finalizado el proceso de copia, digitalización o envío.
- Asegurarse de que la documentación digitalizada mediante las herramientas de escaneo corporativas se aloja en el directorio compartido donde habrán de almacenarse las imágenes obtenidas y no en otro.
- Asegurarse que quede garantizada la confidencialidad de la información contenida en los dispositivos cuando sean devueltos de modo definitivo o entregados a los servicios de soporte para su reparación.
- Obligación de la plantilla fiscales y de funcionarios de notificar sin dilación cualquier incidente que pueda suponer la destrucción, pérdida o alteración accidental o ilícita de los datos personales o la comunicación o acceso no autorizado a dichos datos. La plantilla ha de notificarlo a la jefatura y esta al DPD del MF y a la Unidad de Apoyo de la Fiscalía General del Estado.

4.12.2. Por otro lado, la plantilla de fiscales y funcionarios están obligados a conocer y cumplir las pautas de seguridad que las correspondientes administraciones prestacionales como proveedores de los medios y aplicaciones informáticas, hayan establecido para su utilización [apartado 7.3 e) Instrucción FGE 2/2019]

Los usuarios son los responsables últimos de la seguridad e integridad de los equipos y dispositivos que se les suministran. Por tanto, deberán cumplir con las medidas de protección que establezcan las administraciones prestacionales que los faciliten a fin de proteger la información que contienen, así como para no poner en riesgo a aquella que figure en el sistema en que se integren.

Entre otras, habitualmente se encuentran las siguientes:

- Utilizar el equipamiento suministrado para el uso propio del desempeño profesional.
- Evitar que los equipos o dispositivos sean usados por terceras personas no autorizadas.
- Almacenar en el equipo o dispositivo aquella información indispensable para el desarrollo de las funciones profesionales, procediendo a su borrado cuando ya no sea necesario su tratamiento.
- No habilitar la función de autoguardado de credenciales para acceder a los sistemas de información proporcionados por la administración prestacional.
- Proteger adecuadamente las credenciales de acceso (usuario y contraseña) o de cualquier otro autenticador que permita el acceso a los sistemas de información y cuentas de correo electrónico.
- Desactivar la comunicación Bluetooth del dispositivo cuando no se necesite.
- Asegurar el equipo portátil cuando el usuario se ausente de su puesto de trabajo.
- Notificar a la mayor brevedad al CAU (Centro de Atención al Usuario) si se detecta o sospecha que el equipo o dispositivo ha podido ser manipulado, robado, perdido u objeto de cualquier tipo de vulneración.
- No manipular, desactivar, o modificar la configuración o los sistemas de seguridad instalados (claves, antivirus, firewall o parches de seguridad instalados, etc.).

- No aumentar el nivel de privilegios de su usuario en los sistemas de información empleados, así como su intento.
- No copiar, leer o modificar datos personales almacenados en soportes informáticos de otros usuarios.
- No agregar o quitar componentes de hardware (disco duro, tarjeta de red, etc.).
- No instalar programas sin autorización ni componentes adicionales de los programas instalados, como son componentes del navegador web o codecs para video y audio, etc.
- No manipular o modificar los registros (logs) que genere el sistema operativo y/o las aplicaciones informáticas.
- Realizar conexiones periódicas a la red corporativa, según las instrucciones proporcionadas por la unidad tecnológica correspondiente, para que el equipo o dispositivo se mantenga correctamente actualizado.
- Seguir las pautas de seguridad de las campañas de formación y concienciación impartidas por las administraciones prestacionales en materia de riesgos y uso seguro de las aplicaciones y del acceso a Internet.
- No acceder a páginas web de incierta reputación.
- No abrir correos sospechosos que puedan suponer una amenaza, avisando de ello al correspondiente Centro de Atención al Usuario (CAU) para que los equipos técnicos puedan adoptar medidas de prevención.
- No descargar archivos ni acceder a enlaces contenidos en direcciones de correo que no sean de confianza.

En el caso de uso de equipos particulares, se deberán cumplir además las siguientes medidas de seguridad:

- Notificar a la compañía de telefonía móvil la pérdida o robo del dispositivo a la mayor brevedad posible, así como al CAU para que proceda a desactivar los servicios corporativos ofrecidos desde el dispositivo.
- Evitar la instalación de aplicaciones de origen desconocido o no confiable.
- En caso de ser necesaria la conexión de un dispositivo a un ordenador personal, para su recarga o actualización, no se deberá realizar en equipos de terceros que no sean de confianza.
- Con el fin de evitar el acceso no autorizado, los dispositivos deberán tener activado el bloqueo mediante contraseña, PIN, o cualquier otra característica ofrecida por el dispositivo, tanto para su arranque como para después de un período de inactividad.
- La comunicación, transmisión de información y acceso remoto se realizará únicamente a través de las aplicaciones y canales establecidos, siguiendo los procedimientos y requisitos definidos para ello y adoptando precauciones tales como utilización de contraseñas robustas y cierre de la sesión al terminar la actividad.
- Realizar las actividades de teletrabajo en un espacio que permita la privacidad adecuada a la actividad a realizar (uso de información reservada o confidencial, datos de carácter personal, etc.).

En cuanto a las medidas de seguridad fuera de los centros de trabajo y de entornos seguros**,** dado el riesgo de pérdida o robo de los equipos móviles y portátiles, se han de adoptar las siguientes medidas de precaución:

- Vigilancia permanente. Los dispositivos portátiles y móviles deberán estar vigilados y bajo control para evitar extravíos o hurtos que comprometan la información almacenada o que pueda extraerse de los mismos.
  El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.
- Redes Inseguras. Utilizar la conexión a Internet del domicilio mediante cable directamente conectado al *router* o mediante la red Wifi siempre que ésta esté configurada en modo seguro y con una contraseña robusta. Las conexiones desde lugares públicos se realizarán con la mayor cautela y precaución. Evitar conectar los equipos a redes Wifi abiertas, públicas o desconocidas que, como norma general, son consideradas inseguras.
- Transporte seguro. Los equipos móviles y portátiles fuera de los centros de trabajo se transportarán de manera segura, evitando proporcionar información sobre el contenido en los mismos y utilizando, en su caso, soportes de seguridad que eviten el acceso no autorizado.
  En los desplazamientos se evitará facturar este tipo de equipamiento, que viajará siempre con el usuario.
- Credenciales no visibles. Evitar anotar credenciales de acceso en soportes que puedan ser directamente legibles en caso de pérdida o sustracción.
- Mantenimiento y actualización de los equipos. Cuando se encuentren fuera de los centros de trabajo, los dispositivos móviles y portátiles corporativos se actualizarán atendiendo a las especificaciones técnicas proporcionadas por la correspondiente unidad tecnológica.

4.13 Brechas de seguridad

El RGPD establece en sus arts. 33 y 34, respectivamente, la obligación del responsable de notificar una brecha de seguridad de los datos personales a la autoridad de control (en el plazo de 72 horas a contar desde el instante que se haya tenido conocimiento de ella) a menos que sea improbable que entrañe un riesgo para los derechos y libertades de los interesados, así como el deber de comunicarlo sin dilaciones indebidas a los interesados cuando este riesgo sea alto. La LO 7/2021, establece en sus arts. 38 y 39 unas obligaciones semejantes.

De los citados preceptos se desprenden otras obligaciones como la necesidad de documentar internamente el incidente, así como adoptar medidas para mitigar los daños que se hayan podido producir y aquellas que sean necesarias para evitar que se reproduzcan.

Todo ello constituye una muestra del principio de responsabilidad proactiva por parte de los responsables (art.5.2 del RGPD).

En cuanto a presuntos incidentes de seguridad la Instrucción FGE 2/2019 establece que:

- En caso de que se produzca, en el estricto ámbito de competencias de la jefatura del órgano fiscal o fiscalía, cualquier incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos, debe notificarlo sin dilación al DPD del MF o adjunto del DPD y a la Fiscalía General del Estado [apartado 7.3.i)].

- Los adjuntos territoriales del DPD deberán comunicar al DPD las incidencias que se produzcan en su ámbito territorial (apartado 8.2.4.4).

- La Fiscalía General del Estado deberá recibir la información sobre presuntos incidentes de violación de seguridad, valorar y, en su caso, proceder a comunicar el incidente a la autoridad de control y al interesado. Concretamente corresponderá a la Unidad de Apoyo recibir la información sobre esos presuntos incidentes y comunicar los mismos a la autoridad de control, así como al interesado, en el supuesto de que por la/el Fiscal General del Estado así haya sido decidido (apartado 7.2).

Se ha de tener en cuenta que en caso de que la brecha haya producido como consecuencia de un tratamiento de datos personales con finalidad jurisdiccional la comunicación deberá de dirigirse a la Unidad de Protección de Datos del Ministerio Fiscal una vez esta entre en funcionamiento.

- La notificación a los interesados únicamente se habrá de llevar a efecto siempre que dicho incidente suponga un alto riesgo para los derechos y libertades de las personas físicas cuyos datos se hayan podido ver afectados, notificación que no debiera llevarse a efecto en caso de concurrir alguno de los supuestos contemplados en los apartados 3 y 5 del art. 39 de la LO 7/2021 y fundamentalmente para impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales, o para evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.

- Cuando la brecha de seguridad suponga un alto riesgo para los derechos y libertades de las personas físicas se produzca como consecuencia del ejercicio de la labor que el Ministerio Fiscal desarrolla ante órganos judiciales se considera aconsejable, dadas las posibles implicaciones en la tramitación de los procedimientos, que se informe de ello a los juzgados o tribunales a fin de coordinar las actuaciones a realizar.

- Las anteriores actuaciones deberán realizarse sin dilaciones de modo que permitan una pronta y adecuada toma de decisiones.

ANEXO I

INFORMACIÓN DE DERECHOS RELATIVOS A LA PROTECCIÓN DE DATOS PERSONALES

Finalidad y base jurídica	Sus datos personales serán objeto de tratamiento como consecuencia de la misión y funciones encomendadas al Ministerio Fiscal (art. 124 CE, 1 y 3 del EOMF y concordantes; arts. 6.1. c), 6.1. e), 9) RGPD; art. 8 LO 3/2018; arts. 1, 2, 4 y 13 LO 7/2021)
Responsable del tratamiento	**Ministerio Fiscal** **Añadir:** *el correspondiente órgano fiscal o Fiscalía*
Encargado del tratamiento	**Añadir:** *Ministerio de Justicia* ***o,*** *respecto a las comunidades autónomas con competencias transferidas en materia de Justicia, la denominación de la entidad correspondiente.*
Delegado de Protección de Datos (DPD)	fge.delegadoprotecciondatos@fiscal.es
Derecho a solicitar el acceso, rectificación, supresión, limitación a su tratamiento y oposición, en su caso.	Para su ejercicio puede dirigirse a … *(***Añadir:** *órgano Fiscal o Fiscalía y datos de contacto específicos de la misma)* O por medio del formulario obrante en la dirección web: https://www.fiscal.es/ejercicio-de-los-derechos
Tiempo de conservación de los datos	Sus datos personales se conservarán durante el tiempo que requiera la finalidad del tratamiento y el que, en su caso, determinen las disposiciones legales.
Cesión de datos	Sus datos personales estarán a disposición de los distintos órganos que componen el Ministerio Fiscal y únicamente serán cedidos a otros destinatarios para el exclusivo cumplimiento de sus obligaciones legales.
Reclamaciones	Tiene derecho a presentar reclamación ante la autoridad de control u organismo específico de supervisión que resulte competente según la naturaleza del procedimiento que se tramite a raíz de su petición/denuncia/queja. En su caso, con carácter previo podrá dirigirse al DPD del Ministerio Fiscal

Puede consultar información adicional sobre el derecho a la protección de datos en la dirección web: https://www.fiscal.es

ANEXO II

INFORMACIÓN DE DERECHOS RELATIVOS A LA PROTECCIÓN DE DATOS PERSONALES
ACCESO A EDIFICIOS Y SEDES DEL MINISTERIO FISCAL

Finalidad y base jurídica	Registro y control de acceso a edificios y sedes del Ministerio Fiscal. Sus datos serán objeto de tratamiento para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos [art. 6.1. e) RGPD]. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de derechos digitales.
Responsable del tratamiento	**Ministerio Fiscal** **Añadir:** *el correspondiente órgano fiscal o Fiscalía*
Delegado de Protección de Datos (DPD)	fge.delegadoprotecciondatos@fiscal.es
Derecho a solicitar el acceso, rectificación, supresión, oposición o limitación a su tratamiento.	Para su ejercicio puede dirigirse a … *(***Añadir:** *órgano Fiscal o Fiscalía y datos de contacto específicos de la misma)* O por medio del formulario obrante en la dirección web: https://www.fiscal.es/ejercicio-de-los-derechos
Tiempo de conservación de los datos	Un mes a partir de su fecha de registro.
Cesión de datos	Estos datos se encuentran a disposición de los órganos fiscales que integran el Ministerio Fiscal (art. 22.1 EOMF) para el ejercicio de sus funciones y exclusivamente para el cumplimiento de las obligaciones derivadas de la finalidad referida. Se podrán ceder datos a las autoridades competentes al amparo del art. 6.4 y 23.1 RGPD (supuestos entre los que se encuentran razones de seguridad pública, prevención e investigación de delitos y sanidad pública).
Reclamaciones	Tiene derecho a presentar reclamación ante la AEPD. Con carácter previo a ejercitar ese derecho podrá dirigirse al DPD del Ministerio Fiscal

Puede consultar información adicional sobre el derecho a la protección de datos en la dirección web: https://www.fiscal.es