

**018/2025****I**

El Anteproyecto de ley mencionado (en adelante APL) viene acompañado de la correspondiente Memoria de Análisis de Impacto Normativo (MAIN). Tal y como resulta de la Exposición de Motivos del APL, el objeto de la norma es, en esencia, la transposición de la Directiva (UE) 2023/977 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 relativa al intercambio de información entre los servicios de seguridad y de aduanas de los Estados miembros, por la que se deroga la Decisión Marco 2006/960/JAI del Consejo. Esta norma encuentra su razón de ser en que la actividad de los grupos de delincuencia organizada transnacional es cada vez más una amenaza para la seguridad interior de la Unión Europea y exige una respuesta coordinada, específica y adaptada, y es imprescindible actuar a escala de la Unión Europea para garantizar una cooperación eficiente y eficaz entre los Estados Miembros en lo que respecta al intercambio de información para conseguir estos fines. Esta Directiva (UE) 2023/977 cubre el intercambio de información con fines de prevención, detección o investigación de infracciones penales y establece normas para dicho intercambio de información en las distintas fases de una investigación, desde la fase de recogida de información hasta la fase de investigación penal, incluyendo el intercambio de información a través de Centros de Cooperación Policial y Aduanera. Y dicha norma, en tanto que tal Directiva, ha de ser transpuesta al derecho nacional.

En primer lugar, y desde la perspectiva de la normativa de protección de datos personales, que es lo que a esta AEPD le incumbe en este informe, la Directiva tiene una regulación específica y concreta en materia de protección de datos, que resulta de la finalidad a la que se dirige la norma, y que ha de ser igualmente reflejada en la ley de transposición. Así, como indica efectivamente el art. 3 del APL, este tiene por objeto *establecer medidas destinadas al intercambio de información de manera rápida y adecuada entre los servicios de seguridad y de aduanas de los Estados miembros de la Unión Europea competentes en materia de prevención, detección o investigación de infracciones penales*.

Luego la normativa que regirá los tratamientos de datos personales en esta materia está constituida en España, no por el RGPD y la LOPDGDD, sino por la Ley Orgánica 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, dictada en desarrollo de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (en adelante, Directiva 2016/680). En efecto, el RGPD, en su art. 2.2.d) excluye de la aplicación de esta norma los tratamientos de datos personales *por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.*

El Considerando (23) de la Directiva 2016/680 recoge la importancia de la protección de los tratamientos de datos personales en los intercambios regulados por esta Directiva (y obviamente, por las normas nacionales que la ha de trasponer):

*(23) Resulta especialmente importante que se garantice la protección de los datos personales, de acuerdo con el Derecho de la Unión, en relación con todos los intercambios de información en el marco de la presente Directiva. **Con ese fin, todo tratamiento de datos personales por un punto de contacto único o un servicio de seguridad y de aduanas competente en virtud de la presente Directiva debe llevarse acabo de plena conformidad con lo dispuesto en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo.** De conformidad con el Reglamento (UE) 2016/794, la Agencia de la Unión Europea para la Cooperación Policial (Europol) debe tratar los datos de conformidad con las normas establecidas en él. Dicha Directiva y dicho Reglamento no se ven afectados por la presente Directiva. En particular, se debe especificar que todos los datos personales que intercambien los puntos de contacto único y los servicios de seguridad y de aduanas competentes sigan limitándose a las categorías de datos por categoría de interesado enumeradas en la Sección B del anexo II del Reglamento (UE) 2016/794. En consecuencia, debe establecerse una clara distinción entre los datos relativos a los sospechosos y los datos relativos a testigos, víctimas o personas pertenecientes a otros grupos, a los que se aplican limitaciones más estrictas. Asimismo, en la medida de lo posible, todos estos datos personales deben distinguirse en función de su grado de exactitud y fiabilidad. Con el fin de garantizar la exactitud y fiabilidad, los hechos deben distinguirse de las evaluaciones personales. El punto de contacto único o, cuando proceda, los servicios de seguridad y de aduanas competentes deben tratar las solicitudes de información*

*conformes con la presente Directiva tan rápidamente como sea posible para garantizar la exactitud y fiabilidad de los datos personales, evitar la duplicación innecesaria de los datos y reducir el riesgo de que dichos datos queden obsoletos o dejen de estar a disposición del servicio. Si se observa que los datos personales son incorrectos, deben rectificarse o suprimirse o su procesamiento debe restringirse sin demora.*

Otros Considerandos adicionales (como el 34, relativo al sistema de gestión de casos, que comentaremos separadamente) hacen referencia a la normativa de protección de datos, que, en esta materia, al tratarse de remisión de información en materia “penal”, o la existencia en la actualidad de una “multiplicidad de canales de comunicación” utilizados para la transmisión de información policial entre las autoridades de los distintos Estados miembros, lo que “eleva el riesgo” de la seguridad de los datos personales (Considerando 26).

El Supervisor Europeo de Protección de Datos emitió su informe sobre el Proyecto de Directiva, en Dictamen 5/2022, de 7 de marzo de 2022 (ver Considerando 38).

## II

Entrando ya en el texto del APL, en la definición de “información disponible” (art. 2, letra e) APL), se sugiere que se siga exactamente la redacción del art. 2, apartado 5, de la Directiva 2023/977, para evitar interpretaciones equivocadas respecto de este término. Así, de la redacción del APL podría considerarse (erróneamente) que “información disponible” es aquella que es accesible, a la vez, directa e indirectamente, que no es, ciertamente, ni lo querido por la Directiva ni por el APL. Por eso se considera que debería de redactarse conforme al art. 2.5 Directiva.

En el art. 3 APL, se sugiere que se redacten de nuevo los tres apartados del precepto, de manera que en todos ellos exista un sujeto de la oración que evite la ambigüedad. Así, en el apartado 1 faltaría el sujeto (por ejemplo, “La presente ley no será aplicable [...]”); en el apartado 2 faltaría igualmente el sujeto: (La presente ley se aplicará [...]); y en el apartado 3 se sugiere que se redacte en estilo directo, con el sujeto en primer lugar, y completar: (“La información obtenida como consecuencia de la aplicación de esta ley no podrá usarse en procesos judiciales sin consentimiento expreso del Estado que haya facilitado la misma” -o redacción similar-).

Sobre el art. 6 APL, punto de contacto único, ver comentario respecto del sistema de gestión de casos en el epígrafe III de este informe.

El art. 7 APL, al señalar que *el intercambio de información se llevará a cabo a través de cualquiera de los canales seguros normalizados existentes de cooperación policial y aduanera de la Unión Europea*, parece, al menos en principio, incongruente con (i) el art. 17.1 APL, que dice, en su regla general, que *En todas las comunicaciones previstas en esta ley se utilizará la Aplicación de la Red de Intercambio Seguro de Información de Europol (SIENA)*, y (ii) el propio art. 13.1 Directiva 2023/977: *Los Estados miembros garantizarán que su punto de contacto único o sus servicios de seguridad y de aduanas competentes utilicen la Aplicación de la Red de Intercambio Seguro de Información de Europol (SIENA, por sus siglas en inglés) para enviar solicitudes de información, facilitar información con arreglo a dichas solicitudes o facilitar información de oficio con arreglo a los capítulos II o III o al artículo 12.*

En el art. 12.1 APL se sugiere que se añada el adverbio “Únicamente”, tal y como recoge el art. 6.1 Directiva 2023/977, para reflejar adecuadamente que se trata de una lista cerrada de casos en que se puede denegar la información solicitada: “Únicamente podrá denegarse el acceso [...]”.

En el art. 12.2 se pone de manifiesto un término que no está definido expresamente en la Directiva 2023/977, como es el de “autoridades competentes”. El APL ha elegido la expresión “autoridades competentes” en el art. 5 para referirse expresamente -con otra denominación y sin referirse a ellos como tal- a lo que la Directiva 2023/977 denomina «servicios de seguridad y de aduanas competente». El término “autoridad competente” no está definido en la Directiva, ni tampoco en el art. 2 APL. Se considera que, en tanto en cuanto se refiera exclusivamente dicho término a las autoridades españolas -como hace el art. 5 APL- no habría problema en cuanto a su interpretación. Pero en el art. 12 APL se utiliza de manera diferente al art. 5 APL, para referirse en realidad a los «servicios de seguridad y de aduanas competente» de terceros Estados, término esté sí definido en la Directiva. Se sugiere que se modifique el término utilizado en el art. 12.2 APL, pasando a denominarse «servicios de seguridad y de aduanas competente» (en vez de “autoridades competentes”). Se sugiere igualmente que en el art. 5 se haga una referencia a que las “autoridades competentes” españolas que allí se recogen son los “«servicios de seguridad y de aduanas competentes» a que hace referencia el art. 2, apartado 1), de la Directiva, y el art. 2, letra a), APL designados por España. Obsérvese que, por ejemplo, en el art. 14.1, párrafo segundo, y art. 14.2 APL, no se denominan “autoridades competentes españolas”, sino “servicios de seguridad y de aduanas españoles” (y simultáneamente sí que se denominan “autoridades competentes” a las extranjeras en el mismo art. 14.2 APL. Sería conveniente unificar la denominación, posiblemente bajo la denominación de “servicios de seguridad y de aduanas” por ser la usada por la Directiva.

En el art. 16 se sugiere reemplazar la expresión “si es necesario enviar a Europol” por la de “si procede enviar a Europol”, por ser más exacta, y es además la que utiliza la Directiva en su art. 12.1. Además, el art. 16,

adecuadamente, recoge el Considerando (25) de la Directiva, en cuanto a los casos en que los Estados miembros no están obligados a remitir información a Europol, si bien se sugiere que la redacción del precepto (art. 16.2 APL) se adecúe a la redacción del Considerando 25, que dice así: *Los Estados miembros no deben estar obligados a enviar a Europol una copia de la solicitud de información o de la información intercambiada cuando ello sea contrario a los intereses **esenciales** de la seguridad del Estado miembro de que se trate, cuando **pueda comprometer el éxito** de una investigación en curso o la seguridad de una persona, o cuando revele información relativa a organizaciones o actividades específicas de inteligencia **en el ámbito** de la seguridad nacional.*

Se sugiere que se modifique la redacción del art. 17.2 APL para recoger el sentido del art. 13.3 Directiva. Este último dice que *Los Estados miembros garantizarán que su punto de contacto único y todos los servicios de seguridad y de aduanas competentes que pudieran estar involucrados en el intercambio de información con arreglo a la presente Directiva, estén directamente conectadas a SIENA, en su caso, también desde dispositivos móviles.* No se entiende la expresión “A los efectos de esta ley” que incorpora el texto del art. 17.2 APL, que se sugiere que se suprima por innecesaria. Por otra parte, el art. 17.2 APL usa el término “autoridades competentes señaladas”, cuando el art. 5 APL utiliza la expresión, más acorde con la Directiva, de “designadas”, no siendo “señaladas” un término definido en el APL, por lo que se sugiere su modificación.

### III

El art. 18 APL regula el sistema de gestión de casos, recogido en la Directiva 2023/977 en su art. 16.

En el apartado 1 del art. 18 APL esta AEPD sugiere que se exponga quién va a gestionar o dónde se va a establecer el sistema de gestión de casos, tanto para (i) determinar su ubicación administrativa, ya que el art.16 Directiva establece en términos afirmativos que la implantación y puesta en marcha del sistema de gestión de casos corresponde al punto de contacto único, como (ii) para, en el ámbito del tratamiento de los datos personales, establecer con claridad quién el responsable del tratamiento. No parece haber dudas de que esa cualidad le corresponde a la Secretaría de Estado de Seguridad, ya que el art. 6 APL así lo establece. Por ello se sugiere que la frase del art. 18 APL sea expresa en el sentido de que “se creará en la Secretaría de Estado de Seguridad un sistema único de gestión de casos electrónico [...]” o frase similar.



Se sugiere, además, en el art. 6.2 APL se incluya entre las funciones del punto de contacto único -la Secretaría de Estado de Seguridad-, un nuevo apartado recogiendo que esta será el *responsable del tratamiento* de los datos personales incluidos en el sistema de gestión de casos, con lo que se daría así cumplimiento a lo que regula el art. 3.8 de la LO 7/2021, que define «responsable del tratamiento» o «responsable»: *la autoridad competente que sola o conjuntamente con otras determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión o del Estado miembro, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho de la Unión o del Estado miembro*. En este caso, al fijar tanto la Directiva como el APL que el punto de contacto único es quien gestiona el sistema de registro, tal cualidad de responsable de los tratamientos que lleva a cabo el punto de contacto único, como, entre ellos, expresamente, los tratamientos derivados del sistema de gestión de casos creado por la Directiva, corresponde a la Secretaría de Estado de Seguridad. Por otra parte, de los tratamientos de datos personales que lleven a cabo las distintas “autoridades competentes designadas” (art. 5 APL) serán responsables de los tratamientos cada una de estas autoridades competentes designadas, y sería recomendable igualmente hacerlo constar así.

En el art. 18.1.h) del APL esta AEPD sugiere que se añada, al final de la frase, el inciso “*registrar los accesos y otras operaciones de tratamiento en relación con la información incluida en el sistema de gestión de casos, a efectos de la rendición de cuentas y la seguridad informática, de conformidad con lo dispuesto en el artículo 33 de la Ley Orgánica 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*” para asegurar la concordancia con el art. 16.1.h) de la Directiva, que establece específicamente que la llevanza de dicho sistema de gestión de casos se ha de llevar conforme al “Registro de operaciones” como se regula en el art. 25 de la Directiva (UE) 2016/680, transpuesta en España en el art. 33 de la citada Ley Orgánica 7/2021.

En la frase inicial del art. 18.2 APL se sugiere que la expresión “En este registro (...)” se sustituya por la de “*En este sistema de gestión de casos (...)*”.

El art. 18.3 APL regula el plazo de conservación de los registros en el Sistema de gestión de casos, estableciendo un plazo de cinco años. Esta AEPD informa desfavorablemente dicho precepto, por considerar que es contrario al art. 16.3 y 16.4 de la Directiva 2023/977, si la referencia a los “registros” que realiza este apartado 18.3 APL incluye los datos personales de los “interesados” (definidos en el art. 3.1 Directiva 2016/680 y art. 5.1 LO 7/2021) transmitidos y previamente almacenados en el sistema de gestión de casos. Estos preceptos 16.3 y 16.4 Directiva dicen así:

3. Los Estados miembros velarán por que los datos personales únicamente figuren en el sistema de gestión de casos durante el tiempo que sea necesario y proporcionado para que el punto de contacto único lleve a cabo las funciones que se le asignan en virtud de la presente Directiva y por que los datos personales que figuran en él se supriman posteriormente de forma definitiva.

4. Los Estados miembros velarán por que sus puntos de contacto único revisen, por primera vez a más tardar seis meses después de que haya concluido el intercambio de información y, posteriormente, de forma periódica, el cumplimiento de lo dispuesto en el apartado 3.

Pero a su vez, estos preceptos han de ser interpretados conforme a los Considerandos 23 y 34 de la propia Directiva 2023/977, que establece asimismo la visión del legislador europeo sobre la protección de datos en el ámbito de la Directiva, y aún más específicamente en el aspecto concreto, dentro del régimen de protección de datos, del tratamiento de datos en el sistema de gestión de casos.

(23) Resulta especialmente importante que se garantice la protección de los datos personales, de acuerdo con el Derecho de la Unión, en relación con todos los intercambios de información en el marco de la presente Directiva. Con ese fin, **todo tratamiento de datos personales por un punto de contacto único o un servicio de seguridad y de aduanas** competente en virtud de la presente Directiva debe llevarse a cabo **de plena conformidad con lo dispuesto en la Directiva (UE) 2016/680** del Parlamento Europeo y del Consejo). De conformidad con el Reglamento (UE) 2016/794, la Agencia de la Unión Europea para la Cooperación Policial (Europol) debe tratar los datos de conformidad con las normas establecidas en él. **Dicha Directiva** y dicho Reglamento **no se ven afectados por la presente Directiva**. En particular, se debe especificar que todos los datos personales que intercambien los puntos de contacto único y los servicios de seguridad y de aduanas competentes sigan limitándose a las categorías de datos por categoría de interesado enumeradas en la Sección B del anexo II del Reglamento (UE) 2016/794. En consecuencia, debe establecerse una clara distinción entre los datos relativos a los sospechosos y los datos relativos a testigos, víctimas o personas pertenecientes a otros grupos, a los que se aplican limitaciones más estrictas. Asimismo, en la medida de lo posible, todos estos datos personales deben distinguirse en función de su grado de exactitud y fiabilidad. Con el fin de garantizar la exactitud y fiabilidad, los hechos deben distinguirse de las evaluaciones personales. **El punto de contacto único** o, cuando proceda, los servicios de seguridad y de aduanas competentes **deben tratar las solicitudes de información conformes con la presente Directiva tan rápidamente como sea**

**posible** para garantizar la exactitud y fiabilidad de los datos personales, evitar la duplicación innecesaria de los datos y reducir el riesgo de que dichos datos queden obsoletos o dejen de estar a disposición del servicio. Si se observa que los datos personales son incorrectos, deben rectificarse o suprimirse o su procesamiento debe restringirse sin demora.

**(34) Las normas establecidas en la Directiva (UE) 2016/680 se aplican al tratamiento de datos personales en el sistema de gestión de casos.** El tratamiento incluye el almacenamiento. En aras de la claridad y de la protección eficaz de los datos personales, **las normas establecidas en dicha Directiva deben especificarse con más detalle en la presente Directiva.** En particular, por lo que respecta al requisito establecido en la Directiva (UE) 2016/680 de que los datos personales se conserven en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que son tratados, la presente Directiva debe especificar que, cuando un punto de contacto único reciba información intercambiada en virtud de la presente Directiva que contenga datos personales, **el punto de contacto único solo debe conservar los datos personales en el sistema de gestión de casos en la medida en que sea necesario y proporcionado para el desempeño de sus funciones en virtud de la presente Directiva.** Cuando deje de ser así, **el punto de contacto único debe suprimir irrevocablemente los datos personales del sistema de gestión de casos.** A fin de garantizar que los datos personales solo se conserven durante el tiempo necesario y proporcionado, de conformidad con las normas relativas a los plazos de conservación y revisión establecidas en la Directiva (UE) 2016/680, el punto de contacto único debe **revisar periódicamente** si se siguen cumpliendo esos requisitos. Por ello, debe realizarse una primera revisión a más tardar seis meses después de que un intercambio de información en virtud de la presente Directiva haya concluido, es decir, después del momento en que se haya facilitado el último elemento de información o se haya intercambiado la última comunicación al respecto. No obstante, los requisitos de la presente Directiva relativos a dicha revisión y supresión no deben afectar a la posibilidad de que las autoridades nacionales competentes en materia de prevención, detección e investigación de infracciones penales conserven los datos personales **en sus expedientes penales nacionales con arreglo al Derecho nacional**, de conformidad con el Derecho de la Unión, en particular la Directiva (UE) 2016/680.

Consecuencia de todo lo anterior es que la conservación (tratamiento de datos personales) de los datos personales en el sistema de gestión de casos por un plazo de cinco años es manifiestamente desproporcionado para el cumplimiento de la misión de este sistema de gestión de casos conforme a la



Directiva 2023/977, que no es otro que *facilitar y garantizar el intercambio adecuado y rápido de información entre los servicios de seguridad y de aduanas competentes de los distintos Estados miembros* (Considerando 8, 16 o 18 entre otros).

La Directiva no se opone, en cambio, a que conforme a la legislación nacional de cada Estado Miembro, se conserven dichos datos “*en sus expedientes penales nacionales con arreglo al Derecho nacional*”, de conformidad con el Derecho de la Unión, en particular la Directiva (UE) 2016/680, transpuesta en España por la LO 7/2021, pero no en el sistema de gestión de casos, cuya finalidad es específica, e intermediaria para facilitar la rápida comunicación y tramitación de las solicitudes entre los distintos servicios de seguridad y de aduanas de los Estados miembros.

Por otra parte, en el APL no se recoge en el art. 18 una garantía específica que requiere la Directiva 2023/977 en el citado art. 16.4, que es que el responsable del tratamiento del punto de contacto único deberá proceder, por primera vez en los primeros seis meses, y después de forma periódica, en todo caso a revisar que los datos personales almacenados en el sistema de gestión de casos no figuran en él más tiempo del necesario para que el punto de contacto único lleve a cabo las funciones que se le asignan en virtud de la presente Directiva, y que posteriormente se supriman de forma definitiva.

Así, de esto se desprende lo siguiente:

En primer lugar, el responsable del tratamiento del punto de contacto único deberá llevar a cabo periódicamente, y la primera vez a más tardar seis meses después de *cada* intercambio de información, una revisión para comprobar que se ha cumplido el plazo de conservación y de que los datos se han suprimido definitivamente del sistema único de gestión de casos. La redacción del art. 16.4 Directiva así lo indica, al mencionar la expresión “después de que haya concluido el intercambio de información”, luego esa revisión a más tardar en los primeros seis meses y luego periódicamente ha de realizarse para *cada* intercambio de información en que intervenga el punto de contacto único, de manera que los datos no figuren en el sistema de gestión de casos durante más tiempo del necesario y proporcionado para el fin de este sistema.

En segundo lugar, debe garantizarse en el APL que los datos intercambiados por el punto de acceso único y almacenados en el sistema de gestión de casos son suprimidos posteriormente de forma definitiva de dicho sistema de gestión. Esta garantía no se menciona en el APL, y debe trasponerse. Ello no obsta, por otra parte, como señala la Directiva, que se puedan conservar, conforme al derecho nacional, en los expedientes penales de donde provenían antes de ser remitidos al punto de contacto único.

Por supuesto, ello no obsta tampoco a que la autoridad de control correspondiente haya de ejercer sus competencias y funciones sobre dichos datos, pues como ya se ha expuesto, el art. 18.2.h) APL debería de darse nueva redacción, completándola con la referencia al art. 33 de la LO 7/2021, tal y como hace el art. 16.1.h) Directiva 2023/977 en referencia al art. 25 de la Directiva 2016/680, de manera que

En definitiva, debería de redactarse el art. 18 APL de manera que recogiera expresamente las garantías establecidas en la Directiva al respecto, ya expuestas.

#### **IV**

El art. 19 APL, que es el artículo único del Capítulo V del texto proyectado, regula la Protección de Datos de carácter personal, con un ámbito general.

Su apartado 1 recoge la normativa que según este precepto ha de regir los tratamientos de datos, de una manera a la vez ambigua y, en opinión de esta Agencia, incorrecta. Dice así:

*1. Los tratamientos de datos personales que deriven de la aplicación de esta ley se regirán según corresponda por lo dispuesto en la Ley Orgánica 7/2021, de 26 de mayo, y, en lo que resulte de aplicación, 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 estos datos y por el que se deroga la Directiva 95/46/CE; en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; en la normativa relativa a materias clasificadas; y en sus normas de desarrollo.*

Como se observa mezcla, “para la aplicación de esta ley” (sic) distintas normas, y se sugiere que se redacte de nuevo este apartado haciendo referencia únicamente a la LO 7/2021, porque la Directiva explicita claramente, como ya se ha expuesto, que los tratamientos de datos personales requeridos por el APL, y la Directiva 2023/977 que traspone, tienen como finalidad exclusivamente “la prevención, detección o investigación de infracciones penales” (art. 1.1), materia está expresamente regulada por la Directiva 2016/680 (art. 1.1) y excluida de la aplicación del RGPD (art. 2.2.d) RGPD) y por lo tanto, materia esta igualmente excluida de la aplicación de la LOPDGDD (art. 2.2.a) LOPDGDD).

Una situación similar ya se puso de manifiesto en los apartados 12 a 14 del Informe del Supervisor Europeo de Protección de Datos (SEPD) al proyecto de Directiva (Dictamen 5/2022, de 7 de marzo), citado en el Considerando 38 de la Directiva.

*12. El SEPD también señala que el considerando 16, última frase, establece que las disposiciones de la Propuesta no afectan a las normas de la Directiva sobre la protección de datos personales (LED) ni al Reglamento (UE) 2016/679 (RGPD)<sup>14</sup>. Sin embargo, no queda claro el objetivo de la referencia al RGPD. Según el artículo 2, apartado 1, letra d), del RGPD, este no se aplica al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales.*

*13. Además, el artículo 2, apartado 6, de la Propuesta remite al artículo 4, apartado 1, del Reglamento (UE) 2016/679 para la definición de «datos personales». El SEPD recuerda que la LED contiene una definición idéntica en su artículo 3, apartado 1, que se aplica automáticamente a cualquier tratamiento realizado con arreglo a la Propuesta.*

*14. Por lo tanto, en aras de la seguridad jurídica y la claridad, el SEPD recomienda explicar con mayor claridad en el preámbulo la relación de la Propuesta con el marco jurídico vigente en materia de protección de datos, **y abstenerse de hacer referencia al RGPD, ya que no parece relevante en el contexto del tratamiento de datos personales previsto en la Propuesta.***

(la traducción es nuestra del inglés)

Sugerencia del SEPD que acogió la Directiva 2023/977, pues en ella no se hace referencia alguna al RGPD, sino tan sólo a la Directiva 2016/680, traspuesta en España por la LO 7/2021.

Esta AEPD considera que habría que suprimir asimismo la referencia a la normativa relativa a materias clasificadas, por cuanto esta materia es ajena al APL y a la Directiva que se traspone. El art. 12 APL, en consonancia con el art. 6 Directiva 2023/977, permite denegar la información cuando haya motivos objetivos para creer que la comunicación de la información solicitada podría ser contraria a los intereses fundamentales de seguridad nacional, o perjudicarlos (art. 12, letra f), regla 1ª APL). La Ley 9/1968, de 5 de abril, sobre secretos oficiales, establece en su art. Segundo que podrán ser declaradas "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado. Por lo tanto, estas materias estarían

incluidas en el art. 12.1.f), regla 1ª APL, y sería posible denegar las peticiones de información referidas a ellas, por lo que no habría tratamiento de dichos datos “a los efectos de esta ley”. En cualquier caso, el art. 2.3, letra d) de la LO 7/2021 excluye de la misma los tratamientos sometidos a la normativa sobre materias clasificadas, entre los que se encuentran los tratamientos relativos a la Defensa Nacional.

Esto lleva a una reflexión adicional respecto de este art. 12 APL, y es que se considera que sería más prudente establecer la frase inicial del precepto no como “podrá denegarse”, que parece que hace referencia a una posibilidad tan sólo de denegación, potestativa, cuando en realidad, como se desprende del texto, dicha denegación deviene obligatoria cuando no se dan las condiciones para la transmisión de la información (por ejemplo, y se ve claramente, cuando no hay autorización judicial, de ser esta necesaria); esto es, “Se denegarán”.

El apartado 3 del art. 19 también se considera que deberá modificarse, y hacer una mera remisión a que: **“Las restricciones a los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento se regirán por el artículo 24 de la Ley Orgánica 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”**, como resulta, entre otros, del Considerando 23 Directiva 2023/977, ya transcrito.

Por otra parte, la Directiva 2023/977 no prevé en sí misma un régimen específico, distinto de la Directiva 2016/680 a la restricción al derecho fundamental a la protección de datos de los interesados, sino que se remite con carácter general a la Directiva 2016/680 para los tratamientos de datos personales, en España traspuesta por la LO 7/2021. Es esta la que establece el régimen posible de restricción del derecho fundamental a la protección de datos en el ámbito de la investigación o detección de infracciones penales. En concreto en el art. 24, el cual, como puede observarse, contiene una regulación más completa y específica que el texto del art. 19.3 APL, estableciendo en concreto garantías en caso de restricción (apartado 2), de las que el art. 19.2 carece.

Asimismo, no está de más recordar que la restricción del derecho fundamental ha sido regulada en el art. 24 LO 7/2021 con el carácter de orgánica y que el APL, que establece un régimen diferente para un punto específico (restricción al derecho de acceso), también regulado en el art. 24 LO 7/2021, carecería de rango suficiente para modificarlo.

Por último, en este apartado relacionado con la regulación y trasposición de la normativa prevista de la Directiva sobre datos personales al APL, la

MAIN, en su apartado 4.1, Tabla de correspondencia, señala que el art. 10 de la Directiva se corresponde con el art. 19 del APL. Por la importancia de este tema para este Informe de la AEPD, cabe recordar que el art. 10 de la Directiva establece unas obligaciones concretas para el Estado miembro, que consiste en velar, de una determinada forma, por la protección de datos personales en estos tratamientos concretos regulados en la Directiva, estableciendo unas determinadas garantías específicas en el ordenamiento jurídico nacional.

El art. 10 de la Directiva 2023/977 dice así:

*Artículo 10*

***Normas complementarias para la información que consista en datos personales***

***Cuando el punto de contacto único o los servicios de seguridad y de aduanas competentes de los Estados miembros faciliten información en virtud de los capítulos II o III que consista en datos personales, los Estados miembros velarán por lo siguiente:***

- a ) *que los datos personales sean exactos y completos y estén actualizados, de conformidad con el artículo 7, apartado 2, de la Directiva (UE) 2016/680;*
- b ) *que las categorías de los datos personales facilitados por categoría de interesado se limiten a las que aparecen en la lista del anexo II, sección B, del Reglamento (UE) 2016/794 y sean necesarias y proporcionales para lograr el objetivo de la solicitud;*
- c ) *que su punto de contacto único o sus servicios de seguridad y de aduanas competentes también faciliten, al mismo tiempo y en la medida de lo posible, los elementos necesarios para que el punto de contacto único o los servicios de seguridad y de aduanas competentes del otro Estado miembro puedan evaluar el nivel de exactitud, integridad y fiabilidad de los datos personales, así como la medida en que los datos personales están actualizados.*

No parece haber nada en el art. 19 del APL (como resultaría de la tabla de correspondencia mencionada en la MAIN) que haga referencia a estas garantías específicas para los tratamientos de datos cuando la información que consista o contenga datos personales se facilite a otros Estados, por lo que esta AEPD debe **informar desfavorablemente, por su no inclusión en el APL.**



Por lo que hace a la Memoria de Análisis de Impacto Normativo (MAIN), aportada con el APL, en su apartado 2.3 hace referencia a que *La futura ley resultaría eficaz y eficiente para la consecución de los objetivos que persigue, esto es, **facilitar el uso de información financiera, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales** o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública;* sin embargo se sugiere revisar esta afirmación a la vista del art. 1.2 y del Considerando (10) de la Directiva 2023/977, (...) y específicamente a la norma citada en la Nota 12 a pie de página al Considerando 10.

*Art. 1.2: La presente Directiva **no será aplicable a los intercambios de información** entre los servicios de seguridad y de aduanas competentes con el fin de prevenir, detectar o investigar infracciones penales, **cuando tales intercambios estén específicamente regulados por otros actos jurídicos de la Unión.***

*Considerando (10): Las normas establecidas por la presente Directiva no deben afectar a la aplicación de las normas del Derecho de la Unión relativo a los marcos o sistemas específicos para estos intercambios, como las normas en virtud de los Reglamentos (UE) 2016/794 (7), (UE) 2018/1860 (8), (UE) 2018/1861 (9), y (UE) 2018/1862 (10), del Parlamento Europeo y del Consejo, de las Directivas (UE) 2016/681 (11) **y (UE) 2019/1153 del Parlamento Europeo y del Consejo** (12) y de las Decisiones 2008/615/JAI (13) y 2008/616/JAI del Consejo (14).*

*Nota 12; **Directiva** (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se **establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales** y por la que se deroga la Decisión 2000/642/JAI del Consejo (DO L 186 de 11.7.2019, p. 122)*

Igualmente se sugiere que se revise la afirmación contenida en el párrafo final del apartado 2.4 de la MAIN, cuando dice que [r]especto al rango de la ley, habida cuenta de que se trata de una norma que no afecta al acceso a información sensible **ni afecta a los derechos fundamentales de las personas**, la transposición exige la aprobación de una ley con rango de ordinaria, a la vista del comentario que se realiza en el epígrafe IV de este Informe sobre el apartado 3 del art. 19 APL y la “restricción” que se pretende del derecho de acceso en ese específico precepto, y el carácter de ley orgánica que ya tiene la LO 7/2021.

El párrafo final del apartado 3.4 hace referencia al art. 18, sobre el sistema único de gestión de casos. Una vez revisado este precepto para incluir, en su caso, lo referente a los períodos de conservación de los datos personales

en el sistema único de gestión de casos y la necesidad de revisión del sistema respecto de las solicitudes de información a que se ha hecho referencia en el epígrafe III de este Informe, se sugiere que se complete este apartado 3.4 de la MAIN con esas referencias.

Del mismo modo, el apartado 3.5 MAIN, relativo al Capítulo V APL, que trata precisamente de los datos personales (art. 19 APL), se sugiere su modificación a la vista de las modificaciones que resulten del epígrafe IV de este Informe.

En el apartado 5 B.2, Impacto presupuestario, de la MAIN, al tratar de justificar el “no incremento del gasto”, proclamado de manera esencialmente voluntarista, a la vista de las obligaciones que establece la Directiva (por ejemplo, las de reuniones periódicas previstas en el art. 17.2 o en el Considerando (35) Directiva), en la Disposición Adicional primera, se hace referencia a las “unidades de información de transparencia” existentes en los departamentos ministeriales, que parecen fuera del contexto de la Directiva y del objetivo y finalidad del APL, no estableciéndose en realidad cuál es la función en este APL de esas “unidades de información y transparencia”.

El apartado 5.G de la MAIN hace referencia al Impacto en la protección de datos personales, y extrañamente comienza diciendo que la norma tiene un “impacto positivo” (sic) en materia de protección de datos personales, *“al establecer un medio seguro de transmisión de los datos que, cumplimiento estrictamente con la normativa aplicable, facilita la libre circulación de estos entre autoridades competentes a los fines de prevención, detección o investigación de infracciones penales”*. Esta AEPD considera que dicha expresión es desafortunada e incorrecta, pues toda norma que establece (impone) un tratamiento de datos personales supone una afección al derecho fundamental a la protección de datos personales, que, como es sabido, el TC en su STC 292/2000 estableció que el derecho fundamental a la protección de datos se concreta en un poder de disposición y de control sobre los datos personales. De esta manera, la persona debe quedar facultada para decidir cuáles de sus datos proporcionar a un tercero, sea la Administración o un particular, decidir cuáles puede este tercero recabar, saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Ahora bien, ese derecho fundamental no es absoluto, sino que habrá que ponderar su prevalencia o no en relación con otros derechos o intereses constitucionalmente protegidos. De ahí que el legislador europeo en este caso haya ponderado que un bien digno de protección, como la protección frente a la delincuencia internacional, amerite una afectación al derecho fundamental en los términos establecidos por la Directiva, pero ello no supone en ningún caso un “impacto positivo” en el derecho fundamental. La expresión usada en la MAIN parece confundir la afectación al derecho fundamental, que es el “impacto” cuyo análisis exige que se lleve a cabo en la MAIN, con las medidas que, en relación con las garantías de ese derecho, se establecen en la

Directiva y el APL para paliar esa afectación (o impacto negativo) en el derecho fundamental.

El párrafo segundo de dicho epígrafe 5 G de la MAIN igualmente parece confundir el impacto en el derecho fundamental a la protección de datos con la finalidad a la que dichos tratamientos de datos previstos en la norma se dirigen, que es a favorecer el rápido intercambio de información para la detección, prevención etc. de infracciones penales.

El párrafo tercero del apartado 5G hace una referencia nominativa a normas que ni siquiera son de aplicación a la presente norma, como el Reglamento (UE) 2018/1725, relativo al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión Europea, por lo que no se pretende que cumpla con ningún requisito de la misma; en cuanto a las demás normas citadas en ese apartado, y al pretendido cumplimiento por el APL de ellas, ya se ha hecho referencia, con cita del Informe del SEPD, a que el RGPD no es aplicable en este contexto. Lo mismo, a estos efectos, cabe decir del Reglamento 2016/794 etc.

Esta Agencia no acaba de comprender la afirmación que se realiza en la MAIN de que *“Esta norma no crea un tratamiento o registro de datos nuevos puesto que el instrumento de conexión o intercambio, la Red de Intercambio Seguro de Información-Secure Information Exchange Network Application (SIENA por sus siglas en inglés) ya está establecido y los tratamientos origen o destino a nivel nacional son tratamientos ya establecidos bajo la LOPDP. Al no crearse un nuevo tratamiento en la misma, no es necesario acudir a las recomendaciones de la AEPD”*, pero en cualquier caso discrepa de la misma. Es obvio que la norma (APL) regula tratamientos de datos personales, para lo cual basta dirigir al redactor de la MAIN al art. 5.b) de la LO 7/2021 en cuanto a la definición de *“tratamiento” como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*. Y esta ley regula cuando menos el registro, la organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, acceso, cotejo, interconexión y supresión de datos personales, todos los cuales son operaciones de tratamiento que se producen para el intercambio de información regulado en el APL. Por estas razones, toda la argumentación que se contiene en ese apartado 5 G de la MAIN no responde a la realidad de la norma en su relación con el derecho fundamental a la protección de datos.

Para terminar, el párrafo final del apartado 5G dice así: *Como la norma proviene del legislador europeo, se acomoda a lo previsto por el Alto Tribunal,*

*faculta la libre circulación de los datos personales con fines “policiales” y no crea nuevos tratamientos, no se entiende necesario que se realice una EIPD en cada uno de los tratamientos nacionales que pudieran albergar la información.*

A este respecto esta AEPD no conoce de dónde proviene ni qué norma sustenta esta afirmación, puesto que ni la “proveniencia del legislador europeo” de la norma, ni el que “facult[e] la libre circulación de los datos personales con fines “policiales”, ni por supuesto el que “no cree nuevos tratamientos”, (lo que ya se ha expuesto que no se comparte) son considerados ni por la Directiva 2023/977 ni por la LO 7/2021 (que traspone la Directiva 2016/680), -ni se nombra por la MAIN norma positiva que lo establezca- causa para eximir de una garantía del derecho fundamental a la protección de datos personales como es la realización de una EIPD en los casos en que la norma lo establece. Y en este caso, el art. 35 de la LO 7/2021 establece:

**Artículo 35. Evaluación de impacto relativa a la protección de datos.**

1. Cuando sea **probable** que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, suponga por su naturaleza, alcance, contexto o fines, un **alto riesgo para los derechos y libertades de las personas** físicas, el responsable del tratamiento **realizará, con carácter previo**, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.

2. La evaluación incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos peligros, así como las medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar su conformidad con esta Ley Orgánica. Esta evaluación tendrá en cuenta los derechos e intereses legítimos de los interesados y de las demás personas afectadas

Entre las funciones del Delegado de Protección de Datos se encuentra la de (art. 42.c) LO 7/2021) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización.

Y por último, la LO 7/2021 considera infracción grave (art. 59 I)) El incumplimiento de la evaluación de impacto en la protección de los datos de carácter personal, si se derivan perjuicios o riesgos de carácter grave para los interesados.

En conclusión, en este aspecto se sugiere que se redacte de nuevo, en su integridad, el apartado 5G de la MAIN, con la asistencia del Delegado de Protección de Datos, entre cuyas funciones se encuentra (art. 42 a) LO 7/2021)

*la de Informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del mismo, acerca de las obligaciones que les incumben en virtud de esta Ley Orgánica y de otras disposiciones de protección de datos aplicables.*