La consulta plantea con carácter urgente el parecer de esta Agencia en relación con “los aspectos relativos a la seguridad y garantía de autenticidad e integridad del sistema que presenta la adhesión a este Acuerdo (de Círculo de Confianza en el marco del proyecto europeo e-Codex) desde el punto de vista de la protección de datos de carácter personal y el tratamiento de los mismos. A tal efecto, en la “memoria explicativa” de la consulta que se remite conjuntamente a la misma, se recuerda que el Acuerdo fue objeto de informe de la Abogacía del Estado del Ministerio de Justicia, evacuado el 13 de mayo de 2013 en que, tras concluir que “no se aprecia colisión del proyecto remitido con la normativa nacional o comunitaria”, se indicaba que “se considera oportuna la consulta sobre los aspectos relativos a la seguridad y garantía de autenticidad e integridad del sistema desde el punto de vista de la protección de datos de carácter personal y el tratamiento de los mismos, a la Agencia Española de Protección de Datos”.

Teniendo en cuenta lo anterior, y que el texto que fue informado por la Abogacía del Estado del Ministerio de Justicia es probablemente el que ahora se remite para someterlo al parecer de esta Agencia, toda vez que se indica que el Acuerdo fue adoptado por la Asamblea General de e-Codex el 20 de febrero de 2013, el presente informe se centrará en el análisis de los aspectos de autenticidad y seguridad de la información a los que se refiere la consulta, dado que el informe de 13 de mayo de 2013 ya concluía en la conformidad a derecho del Acuerdo en lo que respecta a los aspectos sustantivos del intercambio de información.

Según se indica en la “memoria justificativa” de la consulta el Proyecto e-CODEX en que se enmarca el Acuerdo objeto del presente informe tiene por objeto “que la comunicación entre los principales actores de la Justicia de los distintos países implicados, se produzca de forma electrónica, garantizando en todo caso la entrega efectiva de la información, sin alteración de su contenido (integridad), de forma segura (cifrada) y garantizando la identidad de los intervinientes (autenticidad)”. Para ello, está prevista la implantación a lo largo del presente mes de un proyecto piloto de asistencia mutua legal que permitirá para los usuarios y sedes judiciales que se den de alta en el piloto, “el envío de

comisiones rogatorias (por el momento sólo en el orden penal) a otros usuarios y sedes judiciales de estados miembros de la Unión Europea que también se hayan dado de alta en el piloto", así como "el envío de los escritos de respuesta correspondientes a las comisiones rogatorias, y otros escritos asociados".

El acceso a esta funcionalidad se verificará a través de Lexnet, seleccionando de la citada herramienta los formularios correspondientes a las comisiones rogatorias.

El Acuerdo de Círculo de Confianza tiene por objeto garantizar la autenticidad e integridad de la información, pudiendo así reconocerse la información como fiable en base a un principio de reconocimiento mutuo, al implantar todos los intervinientes un estándar que, como mínimo cumplirá las garantías de seguridad establecidas en el Acuerdo. Al propio tiempo, las partes que se adhieran al Acuerdo sobre el Círculo de Confianza "deben asegurarse que se adoptan todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar la alteración, pérdida o tratamiento no autorizado o el acceso a dichos datos (en particular la autenticidad y confidencialidad de los datos, y la trazabilidad, integridad, disponibilidad y no repudio de los mensajes)".

El Acuerdo de Círculo de Confianza se fundamenta el establecimiento de un estándar de documento electrónico que deberá reunir los requisitos establecidos en el artículo 1.2 del Acuerdo, acompañado de un comprobante o "token" que incorporará la información que exige el Anexo III, a fin de garantizar el contenido de su información, su evaluación técnica o garantía de la identificación y autenticación del firmante y su validación por el sistema proporcionado por el remitente, de tal forma que no sea precisa su validación posterior en destino y sobre la base del principio de reconocimiento mutuo derivado del cumplimiento del Acuerdo. Para ello se emplearán sistemas electrónicos avanzados bien basados en firma electrónica reconocida, bien en sistemas de autenticación del usuario. El sistema además emitirá para cada envío y recepción evidencias de sellado de tiempo en los términos descritos en el Anexo 5 del Acuerdo.

El apartado 5 se refiere a la protección de datos y a la seguridad, indicando que "Las Partes, a través de sus puntos de contacto y de acuerdo con las leyes de protección de datos a nivel europeo y nacional, deberán adoptar todas las medidas técnicas y organizativas necesarias para garantizar

la seguridad de los datos personales y evitar la alteración o pérdida o tratamiento no autorizado o el acceso a dichos datos (en particular, la autenticidad, confidencialidad de los datos, la trazabilidad, la integridad, la disponibilidad y el no repudio y la seguridad de los mensajes)". Añade que "Tales medidas en la aplicación de la prueba piloto penal deben abordar, como mínimo, las disposiciones de la Decisión marco 2008/977/JAI del Consejo, el artículo 22 § 2", indicando expresamente el texto de febrero de 2013 que dicha Decisión Marco deberá reemplazarse por la Directiva 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 la libre circulación de dichos datos, adoptada finalmente el 27 de abril de 2016 (Directiva (UE) 2016/680), en vigor desde el 5 de mayo de 2016 y respecto de la cual el artículo 63.1 establece como fecha límite de transposición el 6 de mayo de 2018.

Además de las medidas mencionadas, el Anexo 2 establece un proceso de registro de los usuarios, que requerirá su identificación y la exigencia de posterior autenticación mediante un certificado electrónico software, además de un código de usuario y contraseña que vincule unívocamente el documento con el usuario que lo remite.

Las conexiones están, según el Anexo 2 cifradas y securizadas por certificados electrónicos, registrándose todos los mensajes entrantes y salientes y asegurándose la trazabilidad de los documentos enviados. Esta información deberá conservarse por un período de tres meses desde la fecha del mensaje.

Una vez descrito someramente el contenido del Acuerdo y las medidas que el mismo establece procede analizar la conformidad del mismo con las previsiones de reguladoras del derecho fundamental a la protección de datos de carácter personal en lo que se refiere a "los aspectos relativos a la seguridad y garantía de autenticidad e integridad del sistema", tal y como se ha indicado con anterioridad.

Como ya se ha dicho, el Acuerdo se remite al marco del Derecho de la Unión vigente en la materia, que actualmente se configura por 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, cuyo artículo 29 establece lo siguiente:

> "1.Los Estados miembros dispondrán que el responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, sobre todo en lo que se refiere al tratamiento de las categorías especiales de datos personales previstas en el artículo 10.
>
> 2.Por lo que respecta al tratamiento automatizado, cada Estado miembro dispondrá que el responsable o encargado del tratamiento, a raíz de una evaluación de los riesgos, ponga en práctica medidas destinadas a:
>
> a) denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento (control de acceso a los equipamientos);
>
> b) impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas (control de los soportes de datos);
>
> c) impedir que se introduzcan sin autorización datos personales conservados, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización (control del almacenamiento);
>
> d) impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de los usuarios);
>
> e) garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado solo puedan tener acceso a los datos personales para los que han sido autorizados (control del acceso a los datos);

f) garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos (control de la transmisión);

g) garantizar que pueda verificarse y constatarse *a posteriori* qué datos personales se han introducido en los sistemas de tratamiento automatizado y en qué momento y por qué persona han sido introducidos (control de la introducción);

h) impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);

i) garantizar que los sistemas instalados puedan restablecerse en caso de interrupción (restablecimiento);

j) garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema (integridad).”

Por otra parte, y teniendo en cuenta el derecho interno y que el intercambio de datos se llevaría a cabo en el ámbito de la jurisdicción penal, debería tenerse en cuenta que el artículo 81.2 a) del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1726/2007, de 21 de diciembre, establece que “ddeberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los (…) ficheros o tratamientos de datos de carácter personal (…) relativos a la comisión de infracciones administrativas o penales”.

Teniendo en cuenta tanto el marco del derecho nacional como el de la Unión Europea sería preciso valorar si el Acuerdo resultaría conforme con dicho marco en lo que respecta a la seguridad.

A tal efecto, debe recordarse que el propio Acuerdo sobre el círculo de confianza señala en su cláusula 5 que “las Partes, a través de sus puntos de contacto y de acuerdo con las leyes de protección de datos a nivel europeo y nacional, deberán adoptar todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar la alteración o pérdida o tratamiento no autorizado o el acceso a dichos datos (en particular, la autenticidad, confidencialidad de los datos, la trazabilidad, la integridad, la disponibilidad y el no repudio y la seguridad de los mensajes)” y que particularmente “Tales medidas en la aplicación de la prueba piloto penal deben abordar, como mínimo, las disposiciones de la Decisión marco 2008/977/JAI del Consejo, el artículo 22 § 2”. Igualmente se indica de forma expresa que la referencia a la Decisión Marco “deberá reemplazarse por la directiva 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 la libre circulación de dichos datos”; es decir, a la ya adoptada Directiva (UE) 2016/680, de 27 de abril.

De este modo, el propio Acuerdo impone el cumplimiento de las normas de derecho nacional y de la Unión que resulten aplicables en cada momento en materia de seguridad, lo que otorgaría por sí mismo garantías del cumplimiento de esas obligaciones en caso de firma del Acuerdo, sin perjuicio de su posible verificación posterior.

Pero además, el Propio texto del Acuerdo establece en sus Anexos diversas garantías de seguridad que vienen a clarificar que efectivamente se implantarán las mencionadas medidas.

Así, el Anexo 2 prevé la existencia de un proceso de registro de usuarios, previa identificación de los mismos, llevada a cabo en ocasiones por las asociaciones representativas de sus categorías profesionales. Dichos usuarios son objeto de autenticación a través de certificado electrónico, unido al código de usuario y contraseña, quedando además todos estos medios bajo el control del usuario. Además, se establece una limitación de accesos al conector nacional en el anexo 4 del documento.

El acceso al sistema se producirá a través del sistema nacional, entendiendo como tal el sistema LexNet, regulado por el Real Decreto 1065/2015, de 27 de noviembre, ya informado por esta Agencia. Asimismo se

establece la obligación de garantizar la trazabilidad de la información objeto de intercambio, guardándose los registros referidos al intercambio de la información durante un plazo de tres meses. En todo caso, la integridad de los mensajes se garantiza a través de los sistemas de cifrado detallados en el Acuerdo, unidos a los exigidos, en el ámbito interno por el ya mencionado Real decreto 1065/2015. Toda la información referida al intercambio y necesaria para la validación del documento se contendrá igualmente en el comprobante o "token" al que se refiere detalladamente el Anexo 3. Igualmente el Anexo 5 establece los requisitos de sellado de tiempo y los procedimientos de recuperación.

Teniendo todo lo mencionado en cuenta, cabe considerar que las garantías ofrecidas por el Acuerdo de Confianza sometido al parecer de esta Agencia en lo referido los aspectos relativos a la seguridad y garantía de autenticidad e integridad del sistema resulta, en los términos en que se describen en el Acuerdo y sus Anexos, conforme con la normativa vigente en materia de protección de datos de carácter personal.