Se consulta si, conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, para comunicar los datos relativos a los colegiados a los delegados de comunidad autónoma, personas físicas nombradas por la Junta de Gobierno del colegio oficial consultante, para que ejerzan una labor de información a los colegiados es preciso el consentimiento de éstos o si el Colegio debe remitir directamente la información a los colegiados sin previa cesión a los delegados de datos personales. Se plantea también si, en su caso, es necesario que el delegado realice algún documento vinculante por la custodia de los datos facilitados y qué los datos deben ser facilitados a estos efectos (dirección postal, correo electrónico, teléfono). Señala asimismo el consultante que los delegados no tienen sede física y el contacto con los colegiados de su zona se realiza desde su ordenador privado.

Para dar respuesta a las cuestiones planteadas debe tenerse en cuenta que la Ley Orgánica 15/1999 define en su artículo 3.d) al responsable del fichero o tratamiento como la *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.*" De la misma manera el Reglamento de desarrollo de dicha Ley, aprobado por Real Decreto 1720/2007, de 21 de diciembre, define en su artículo 5.1. q) al responsable del fichero o tratamiento como la "*Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente."*

Cabe señalar que la condición de responsable del tratamiento es consecuencia del hecho de que un ente haya decidido tratar datos personales para sus propios fines, correspondiéndole por ello asumir la responsabilidad del cumplimiento de las normas sobre protección de datos. De este modo, la entidad consultante resultará responsable de los ficheros que, conteniendo datos personales, mantiene para el ejercicio de su actividad (entre ellos el de colegiados). Es por tanto el Colegio consultante, esto es la entidad que ha decidido la creación, contenido y finalidad del fichero o ficheros, quien estará sujeta a todas aquellas obligaciones y deberes impuestos por la Ley Orgánica 15/1999 y su normativa de desarrollo, así como a las responsabilidades que conforme a dicha Ley sean exigibles.

Con carácter general será la Junta de Gobierno, a quien se le encomienda la gestión directiva, quien podrá acceder a los datos personales obrantes en el colegio para el ejercicio de sus funciones. En este sentido cabe señalar que en los estatutos se recoge expresamente entre sus funciones la "*de informar a los colegiados con prontitud de cuantas cuestiones puedan afectarles, ya sean de índole corporativa, colegial, profesional o cultural de las que la Junta de Gobierno tenga noticias en el ejercicio de su función o en el de alguno de sus miembros o representantes de ellos*." De este modo el tratamiento de datos personales de los colegiados que lleva a cabo la Junta de Gobierno con dicha finalidad deriva de los propios estatutos.

Del examen de los documentos aportados, Estatutos y Reglamento de Régimen interior, se desprende que pueden existir otros órganos que, igualmente para el ejercicio de sus funciones, puedan precisar tratar datos de los colegiados. Así su artículo 61 señala que la Junta de Gobierno podrá nombrar, si lo considera oportuno, un delegado de la Junta en las Comunidades Autónomas donde no exista delegación cuyas funciones serán las previstas en el Reglamento de Régimen interior. Este delegado, conforme a lo señalado en dicho Reglamento dará cuenta de su gestión institucional y económica a la Junta de Gobierno, a través del Presidente del Colegio o miembros de la Junta de Gobierno en quien este delegue. En cuanto a sus funciones, serán las previstas en el artículo 80 de dicho Reglamento, así como las que "le delegue la Junta de Gobierno del colegio o las actividades que este le demande"

Por consiguiente, no corresponde a esta Agencia determinar si es la Junta de Gobierno o el delegado quien debe relacionarse con los colegiados para remitirles información profesional o de otro tipo, sino al propio consultante, puesto que aun cuando el Reglamento de régimen interior no atribuye expresamente dicha función al delegado, puede serle encomendada por la Junta de Gobierno. En el caso en que se le encomiende tal función no se producirá una cesión de datos sino que, al igual que en el caso de la Junta de Gobierno, el tratamiento de los datos personales de los colegiados derivará de lo establecido en sus estatutos y demás normas de funcionamiento.

De la misma manera, algunas de las funciones reconocidas expresamente al delegado requerirán el tratamiento de datos de determinados colegiados, tratamiento que se enmarca igualmente de lo establecido en las normas de funcionamiento del colegio profesional consultante.

Ahora bien, dichos tratamiento de datos, sean los establecidos en el Reglamento de régimen interior o los que se le encomienden al delegado por la Junta de Gobierno deberán ser respetuosos de los principios contenidos en el artículo 4 de la Ley Orgánica 15/1999, debiendo destacarse aquí los principios de proporcionalidad y finalidad. El artículo 4.1 de dicha Ley establece que "*Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."* Por su parte, el número 2 del mismo artículo dispone que *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos."* Debe aclararse aquí que la Audiencia Nacional partiendo de una interpretación sistemática de este precepto viene considerando la expresión "finalidades incompatibles" como sinónimo de "finalidades distintas".

En el presente supuesto, la finalidad determinada, explicita y legítima del tratamiento a efectuar por el delegado vendría dada bien por el ejercicio de las funciones que le atribuye el Reglamento de régimen interior, bien por el ejercicio de las que le sean delegadas por la Junta de Gobierno, no pudiendo destinarse los datos a una finalidad diferente a éstas, lo que supondría una vulneración de la Ley Orgánica 15/1999. En lo que respecta al principio de proporcionalidad, el delegado solamente podrá tratar los datos personales de los colegiados cuando sea preciso en el ejercicio de sus funciones. En el caso de que entre estas funciones se le encomendase la remisión de información a los colegiados de su ámbito territorial de actuación solamente podrá acceder a los datos de los colegiados de dicho ámbito y dentro de tales datos, aquéllos utilizados por la Junta de Gobierno para remitir tales informaciones.

En lo que respecta a la confidencialidad cabe recordar que el artículo 10 de la Ley Orgánica 15/1999 sujeta al responsable del fichero, esto es al colegio profesional consultante, a un deber de secreto, deber al que se encuentran igualmente sometidos los miembros de cualquier órgano del mismo que, en el ejercicio de sus funciones, deba acceder a datos personales. Dispone dicho artículo 10 que "*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."* El incumplimiento de este deber es constitutivo de infracción de la Ley Orgánica 15/1999.

II

Entre las obligaciones del responsable del fichero se encuentra la de adoptar las correspondientes medidas de seguridad, de conformidad con lo previsto en el artículo 9 de la Ley Orgánica 15/1999, según el cual "*El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural."*

El número 2 de dicho precepto prohíbe el registro de datos de carácter personal en ficheros "*que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas*." El Reglamento de desarrollo de la Ley Orgánica 15/1999, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal.

En el presente supuesto se indica que los delegados van a utilizar sus propios ordenadores privados, lo que plantea tanto problemas respecto de la seguridad de los datos personales que se traten en ellos como respecto a la protección de la privacidad de los propietarios de tales equipos, en tanto que el responsable tiene que adoptar, tal y como señala el artículo 9 las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal.

Esta Agencia ha venido señalando en sus informes que el uso de equipos o dispositivos privados, con carácter general, no garantiza la seguridad de los datos de forma que no se produzcan pérdidas o alteraciones de los datos o accesos indebidos. Así, entre los posibles riesgos cabe mencionar que puede producirse inadvertidamente una cesión de datos a terceros, definida en el artículo 3 i) de la Ley Orgánica 15/1999 como "Toda revelación de datos realizada a una persona distinta del interesado". Este riesgo se produce, por ejemplo, si se utilizan programas peer to peer de modo que un tercero pueda acceder indebidamente a carpetas no protegidas, se instalan en un teléfono móvil o en una tablet aplicaciones que requieran el acceso a los datos obrantes en las mismas o cuando se produce un almacenamiento de los datos en una nube (produciéndose así una comunicación de datos al proveedor del servicio

de cloud computing sin que exista un contrato de encargado del tratamiento conforme a las normas establecidas en el artículo 12 de la Ley Orgánica 15/1999), con el agravante de que en ocasiones la falta de transparencia de los desarrolladores de aplicaciones o de los proveedores de cloud computing no permite conocer si se están produciendo accesos a los datos almacenados en los dispositivos o si el tratamiento en la nube respeta lo establecido en la normativa de protección de datos de carácter personal.

A efectos de eliminar los posibles riesgos que comporta el tratamiento de datos personales en equipos privados cabe recordar lo señalado por el International Working Group on Data Protection in Telecommunications, en su documento de trabajo sobre privacidad y los riesgos de seguridad con el uso de "dispositivos propios" en redes corporativas, adoptado en Berlín en 2014. Dicho documento señala los riesgos que generan las prácticas "Bring Your Own Device" (BYOD) y formula diversas recomendaciones, que pueden ser tenidas en cuenta como buenas prácticas.

Así en primer lugar, se menciona la conveniencia de la realización de una evaluación de impacto en la protección de datos personales, que puede considerarse como un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de las personas cuyos datos se tratan y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminar o mitigar en lo posible aquellos que se hayan identificado. A efectos de facilitar dicha evaluación, en la página web de esta Agencia (www.agpd.es) se encuentra publicada una guía en la que se señalan unas directrices para llevar a cabo la misma.

Dentro de dichas recomendaciones, sin perjuicio del interés que todas ellas tienen, cabe resaltar aquí las relativas a la política, formulada por escrito, de obligaciones de los empleados respecto al uso de los dispositivos propios que incluya como mínimo las normas sobre cuando eliminar de tales dispositivos los datos personales de la organización (esto es los datos personales relativos a los colegiados), la obligación de informar a la empresa de que el dispositivo o los datos personales de la organización almacenados en un dispositivo propio han sido robado o la información comprometida y asegurar que no se produzcan accesos no autorizados a datos personales corporativos almacenados o accesibles a través de dispositivos propios, incluso cuando otros aspectos del dispositivo propio puedan ser utilizados por un tercero autorizado, como un miembro de la familia.

Se recomienda definir la mejoras que requiere la política de seguridad de la organización y la infraestructura técnica para facilitar el acceso de dispositivos propios, entre ellas se incluye la de mejorar la infraestructura de comunicaciones para incluir el cifrado de extremo a extremo para la comunicación con los dispositivos propios o efectuar regularmente copias de seguridad de los datos corporativos almacenados en dispositivos propios.

Las recomendaciones se refieren también a la implementación, prueba y validación de las medidas técnicas que incluyen cortafuegos y aislamiento de procesos en dispositivos propios para impedir que los datos corporativos sean accesibles a través de otras aplicaciones, respetando la privacidad del usuario.

Igualmente se recomienda la adopción de procedimientos para validar la integridad de tales dispositivos propios y confirmar que cumplen con los estándares aceptables definidos, tales como una versión mínima del sistema operativo, tipo de dispositivo, protección con contraseña, cifrado (incluyendo el cifrado del sistema de archivos) y protección actualizada contra el malware. Asimismo, se menciona entre las recomendaciones el de implementar procedimientos para detectar y prevenir el uso de software que esté prohibido por la política de la organización como las aplicaciones de intercambio de archivos, aplicaciones de streaming y aplicaciones peer to peer. Esto debe hacerse de una manera que respete la privacidad de los empleados.

Figura asimismo, entre dichas recomendaciones la relativa a la exigencia de una auditoria adecuada, pertinente y proporcional de las actividades llevadas a cabo en los “dispositivos propios”, en particular, minimizando la necesidad de acceso al espacio de los datos personales del usuario final y de seguimiento de la ubicación de los dispositivos fuera de las horas de trabajo programadas. Se indica que es imperativo que las medidas de seguridad diseñadas para proteger los datos de la organización no violen la privacidad del usuario o de un tercero cuyos datos se encuentren en dicha zona privada del usuario del dispositivo (por ejemplo, libretas de direcciones, bandejas de entrada de correo electrónico privadas, fotos de la familia, etc).

Por último, debe tenerse en cuenta que a partir del 25 de mayo de 2018 resultará de aplicación, conforme a lo dispuesto en su artículo 99.2, 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 (Reglamento general de protección de datos), que adopta un enfoque diferente al establecido en la Ley Orgánica 15/1999 y su normativa de desarrollo en lo que respecta a las medidas de seguridad que el responsable de un fichero debe implementar.

Señala el considerando 83 de dicha norma que " A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Y en su artículo 32, números 1 y 2, dispone lo siguiente respecto de la seguridad del tratamiento:

"*1.Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2.Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

De todo lo expuesto debe concluirse que tratamiento de los datos personales de los colegiados en ordenadores o dispositivos privados de los delegados plantea numerosas dificultades para garantizar su seguridad, de modo que el colegio profesional consultante, como responsable del fichero y al que se imputarán, en su caso, las posibles responsabilidades que pudieran derivar del incumplimiento de la obligación de adoptar las correspondientes medidas de seguridad, deberá implementar cuantas medidas sean necesarias para evitar que con el uso de equipos o dispositivos propios por los delegados se produzcan accesos o tratamientos indebidos de los datos personales o su pérdida o alteración. A estos efectos puede servir de referencia lo señalado en el documento del International Working group on Data Protection in Telecommunications antes reseñado, sin olvidar las nuevas exigencias que en materia de seguridad impone del Reglamento General de Protección de datos.