

0030/2024**I**

El art. 24.1 RGPD, al regular la responsabilidad del responsable del tratamiento establece que este (...) *aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento*. Y, entre dichas medidas, *cuando sean proporcionadas en relación con las actividades de tratamiento (...) se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos*.

Se trata por tanto la presente Política de protección de datos (PDD) de una medida técnica y organizativa en el ámbito de la responsabilidad proactiva del responsable del tratamiento cuyo objeto, según el art. 1 del Proyecto presentado, es *regular la Política de Protección de Datos de la Administración de la Comunidad Autónoma las Illes Balears, para definir, implantar y aplicar coordinadamente un marco de gobierno y actuación que permita la gestión proactiva de la protección de los datos de carácter personal tratados por medios electrónicos y en soporte papel (automatizados y no automatizados) en el contexto de las actividades de tratamiento de datos personales y los sistemas de información de la Administración de la CAIB, de acuerdo con el RGPD, la LOPDGDD y demás normativa vigente en materia de protección de datos personales y derechos digitales*.

Esta AEPD considera muy favorablemente dicha Política de Protección de Datos, por cuanto señala la intención del responsable (en este caso la Administración de la comunidad Autónoma) de dotarse de una herramienta ("medida") que permita tanto a quienes van a tratar efectivamente los datos personales de los interesados, como a estos mismos, conocer las reglas, instrumentos y cautelas que han de tenerse en cuenta en dichos tratamientos. Por lo tanto, esta AEPD, sin perjuicio de los comentarios que a continuación se harán sobre el texto, informa favorablemente el Proyecto presentado.

II

Sin perjuicio de lo anterior, y ya entrando en los comentarios específicos a los distintos apartados del texto, cabe mencionar lo siguiente:

En el párrafo quinto del epígrafe I del Preámbulo sería conveniente transcribir de manera completa el artículo 31.14 del Estatuto de Autonomía de las Illes Balears, ya que la competencia de la comunidad autónoma al respecto es el desarrollo legislativo y la ejecución de la protección de datos de carácter personal específicamente *respecto de los ficheros de titularidad de las Administraciones públicas de la Comunidad Autónoma y los entes u organismos de cualquier clase vinculados o dependientes de éstas*.

En el párrafo tercero del epígrafe IV Preámbulo (y en ocasiones posteriores en que se repite la cita), al referirse al texto del Decreto 12/2023 Decreto 12/2023, de 10 de julio, de la presidenta de las Illes Balears, por el que se establecen las competencias y la estructura orgánica básica de las consejerías de la Administración de la Comunidad Autónoma de las Illes Balears, se menciona la Dirección General de Estrategia Digital y Simplificación Administrativa, cuando, salvo que se haya modificado la denominación, el citado Decreto 12/2023 hace referencia en realidad a la Dirección General de Simplificación Administrativa, Modernización y Administración Digital.

En el art. 4.3, primer párrafo, se hace referencia, en general, a que en el ámbito de la Administración Pública de la Comunidad Autónoma de las Illes Balears las bases jurídicas para el tratamiento de los datos personales son, con carácter general, el cumplimiento de una obligación legal aplicable al responsable del tratamiento (artículo 6.1 c) del RGPD), o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1 e) del RGPD). Esta AEPD no se opone a dicha mención, que se entiende como descriptiva, sin perjuicio de recalcar que la base jurídica de cada tratamiento concreto habrá de especificarse en la norma o acto jurídico que, en cada caso, establezca el tratamiento en sí mismo considerado, y que esta habrá de reflejarse en el correspondiente Registro de Actividades de Tratamiento (RAT) y publicarse en el Inventario de las actividades de tratamiento (como acertadamente se recoge en el art. 11 del Proyecto).

Se sugiere que se suprima el párrafo segundo del apartado 5 del art. 4, que dice: *El «test de compatibilidad de finalidades» recogido en el artículo 6.4 del Reglamento (UE) 2016/679, puede aplicarse tanto a tratamientos que realice un mismo responsable, como en el caso de que estemos ante dos tratamientos que los lleven a cabo diferentes responsables del tratamiento*. En primer lugar, porque dicho “test de compatibilidad” (art. 6.4 RGPD, último inciso) normalmente no será de aplicación a la CAIB, ya que los tratamientos de los que sean responsables se habrán de regir, casi en su totalidad, por lo dispuesto en una norma legal, con lo cual será de aplicación lo que esta disponga respecto de la compatibilidad de fines (art. 6.4, primera frase). En

segundo lugar porque puede llevar a confusión ya que podría interpretarse de manera puramente mecánica como que basta con que dichos fines sean “compatibles” para que otro responsable pueda tratar datos personales para una finalidad distinta a la inicial para los que fueron recogidos, sin mayores requisitos, cuando en realidad haría falta igualmente una base jurídica válida para ese nuevo tratamiento diferente; y por último, porque que esté dicho párrafo en el texto o no, no impide, si se dan las circunstancias legales apropiadas, que dichos datos sean tratados para fines “compatibles”. Y para finalizar, porque dicha frase, de carácter general, deberá ser refrendada en cada tratamiento en particular para determinar si dicho tratamiento para un fin distinto es posible, sin que se considere conveniente que la frase, con el carácter general con que se manifiesta, se mantenga.

Artículo 4 párrafo 7, respecto de la Inteligencia Artificial (IA). Sin perjuicio de que se admite el párrafo, que contiene una manifestación de carácter genérico, se sugiere que se añada que los tratamientos que incorporen o utilicen un sistema de IA deberán de cumplir, con carácter específico, aparte de los requisitos para la protección de datos personales que resulten del RGPD y LOPDGDD, los específicos que resulten (tanto respecto del tratamiento de datos personales como de la propia licitud en sí misma del sistema de IA utilizado), respecto de cada sistema de IA utilizado, con los requisitos previstos, en cada caso, en el recientemente publicado Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) -RIA-. Por ejemplo, el considerando (69) del citado RIA dice: *El derecho a la intimidad y a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, son aplicables cuando se tratan datos personales. Las medidas adoptadas por los proveedores para garantizar el cumplimiento de estos principios podrán incluir no solo la anonimización y el cifrado, sino también el uso de una tecnología que permita llevar los algoritmos a los datos y el entrenamiento de los sistemas de IA sin que sea necesaria la transmisión entre las partes ni la copia de los datos brutos o estructurados, sin perjuicio de los requisitos en materia de gobernanza de datos establecidos en el presente Reglamento. O el art. 2.7, que dice: El Derecho de la Unión en materia de protección de los datos personales, la intimidad y la confidencialidad de las comunicaciones se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento. El presente Reglamento no afectará a los Reglamentos (UE) 2016/679 o (UE) 2018/1725 ni a las Directivas 2002/58/CE o (UE) 2016/680, sin perjuicio del artículo 10, apartado 5, y el artículo 59 del presente Reglamento.*

En el apartado 8 del art. 4, se sugiere que tras la expresión “una vez alcanzadas estas finalidades” se añada “según corresponda conforme a los artículos 22, 32 o concordantes, LOPDGDD” para evitar considerar que la elección que plantea este apartado no está sujeto a condicionantes, pues la elección a llevar a cabo dependerá de cada caso que se plantee en concreto.

En el artículo 6.1, primer párrafo, se sugiere añadir al final de este “(...), *sin perjuicio de que sí aplicaría al propio tratamiento de datos personales conducentes a su anonimización*”.

Se sugiere que la frase inicial del art. 7.1 se redacte así: “1. *Los interesados pueden ejercer ante los responsables de cada tratamiento (según el caso los titulares de los órganos directivos de las consejerías de la CAIB y los órganos directivos asimilados) los derechos de (...)*”

En el párrafo segundo del art. 7.2 se sugiere que se comience así: “*Sin perjuicio del derecho e los interesados a relacionarse, cuando corresponda, ante las administraciones públicas a través de medios no electrónicos (art. 14 ley 39/2015), en la sede electrónica de (...)*”

En el párrafo segundo del art. 7.3 se sugiere que se añada al final del párrafo, conforme al art. 12.3 RGPD: “El responsable informará al interesado de cualquier prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

Se sugiere un párrafo adicional en el art. 7.3, reproduciendo el art. 12.4 RGPD: *Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.*

Art. 7.5: se sugiere añadir en el primer párrafo, al inicio, conforme al art. 12.5 RGPD, que “*La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito*”.

El apartado 8 del art. 7, sobre el “derecho al olvido”, tal y como está redactado, puede inducir a confusión, ya que hace referencia al derecho al olvido ante el gestor del motor de búsqueda, que no es la CAIB. Si bien la redacción es correcta, el supuesto de hecho no se aplicaría a la Administración de las Illes balears, que no es un gestor de motor de búsqueda. En consecuencia, se sugiere que este párrafo tenga una redacción similar al art. 15.1 LOPDGDD: *El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679*

Se recomienda suprimir el párrafo final del art. 7.8, ya que está estableciendo en una norma un supuesto que varía según las circunstancias del caso concreto; esto es, el derecho a la protección de datos prevalecerá sobre el derecho a la libertad de expresión en unos casos, y en otros no, con lo cual este párrafo, que es meramente ilustrativo, no regula en realidad ningún supuesto, sino que expone una circunstancia que habrá de interpretar el juez en cada caso. Si no se desea suprimir, debería de redactarse de modo que recoja que en unos casos prevalecerá el derecho a la protección de datos, y en otros la libertad de información/expresión, según las circunstancias del caso.

Por las mismas razones ya expuestas respecto del derecho al olvido, se sugiere suprimir el art. 9 sobre el derecho a la portabilidad, o en su caso sustituirlo por la redacción del art. 17 LOPDGDD.

En la letra k) del art. 8.5, se reitera lo expuesto sobre la denominación de la Dirección General de Estrategia Digital y Simplificación Administrativa.

Se sugiere comenzar el párrafo segundo del art. 9.2 por: *“Dicho contrato o acto jurídico recogerá las circunstancias del art. 28.3 RGPD, y en particular, deben adoptarse y documentarse (...)”*.

El apartado 3 del art. 9 hacer referencia a cuando estamos ante una actividad regida por la Ley de Contratos del Sector Público, (ley 9/2017, de 8 de noviembre, LCSP). Cabe recordar, y se sugiere que se recoja aquí, lo establecido en el art. 122.2 de esta, que requiere que en aquellos contratos cuya ejecución requiera el tratamiento por el contratista de datos personales por cuenta del responsable del tratamiento, adicionalmente en el pliego se harán constar las circunstancias a) a e) recogidas en dicho precepto (que además tienen la consideración de esenciales a los efectos del art. 211.1.f) LCSP).

Art. 10.1: la referencia a la “minimización de datos” como “medida técnica y organizativa” no es correcta. La minimización de datos es un principio relativo al tratamiento (art. 5.1.c) RGPD), pero además lo recoge así también el propio art. 25.1 RGPD referido a la protección de datos desde el diseño y por defecto. Por eso se sugiere modificar la redacción de este precepto para que quede redactado de esta manera, tal y como resulta del art. 25.1 RGPD: *Los responsables del tratamiento deben aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas adecuadas, como la seudonimización, concebidas para aplicar de manera efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, con objeto de cumplir los requisitos del RGPD y de proteger los derechos de los interesados.*

Art. 13.2 (y concordantes en que se cite al “coordinador de protección de datos personales”). No está clara en el proyecto, en opinión de esta Agencia, la relación entre el DPD y el coordinador de protección de datos personales. El art. 35.2 RGPD requiere el asesoramiento del DPD (no de otro órgano o asesor distinto -que ciertamente también podrá existir, pero con carácter adicional, sin sustituir al DPD-). En el art. 15 del proyecto, el coordinador de protección de datos personales parece formar parte de la estructura organizativa de la CAIB, pero como algo diferenciado del DPD, que se regula en el art. 16. Cuando el RGPD requiere el asesoramiento del DPD, ha de ser de esta figura, que está adornada de unas características, independencia y conocimientos requeridos por el RGPD que le hacen idóneo para esta función con entera libertad de criterio. Ello quiere decir que habría de modificarse el texto presentado para que, en todos aquellos casos en que el RGPD requiere el asesoramiento del DPD, se refleje así, por supuesto con independencia de que se decida, además, que la CAIB sea asesorada por otros órganos propios (como estos coordinadores), pero ha de reflejarse que el asesoramiento es aportado por el DPD en todo caso. Debe decirse que la estructura del DPD no necesariamente ha de ser unipersonal; corresponde dicha decisión (unipersonal, colegiado, u otra estructura o funcionamiento; que sea una persona física o una persona jurídica, etc.) al responsable del tratamiento cuando ha de elegirlo, y en este caso, al legislador reglamentario que es quien, en el texto, art. 16, determina la regulación de esta figura en la CAIB.

Art. 14.2; se sugiere añadir una frase adicional, final, que recoja lo establecido a este respecto en el art. 33.1 RGPD: *Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.*

Art.14.5; se sugiere añadir, conforme al art. 34.3 RGPD: *La comunicación al interesado no será necesaria si se cumple alguna de las condiciones señaladas en las letras a) a c) del art. 34.3 RGPD.*

Art. 17.2, apartado 2.2:

- (i) se sugiere, si es posible de una manera fácilmente descriptiva, que se especifique, para la mejor comprensión del lector/destinatario de la norma, qué se entiende por “tratamientos comunes y tratamientos transversales” en los centros docentes públicos no universitarios.
- (ii) No se establece regulación alguna para los tratamientos comunes y transversales de los centros docentes “de régimen especial”, ya que sólo se menciona en este precepto a los de “régimen ordinario”, por lo que en los de régimen especial no se regula quién sería el responsable del tratamiento.

Disposición final primera, apartado 3, del proyecto, por la que se añade un nuevo artículo 20 al Decreto 3/2023. En el apartado 5 del mismo se sugiere que en la letra a) se añada que las contraseñas serán cambiadas periódicamente.