Sección I. Disposiciones generales

CONSEJO DE GOBIERNO

11921 ***Decreto 48/2024, de 22 de noviembre, por el que se aprueba la Política de Protección de Datos Personales de la Administración de la Comunidad Autónoma de las Illes Balears***

Preámbulo

I

La protección de las personas físicas con respecto al tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española, que dispone que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

En este sentido, el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y, por lo tanto, debe mantener el equilibrio con otros derechos fundamentales, de acuerdo con el principio de proporcionalidad.

El artículo 12.3 del Estatuto de Autonomía de las Illes Balears, aprobado por la Ley Orgánica 1/2007, de 28 de febrero, establece que las instituciones propias de la comunidad autónoma de las Illes Balears, para cumplir las finalidades que les son propias y en el marco de las competencias que les atribuye este Estatuto, deben promover, como principios rectores de la política económica y social, el desarrollo sostenible encaminado a la plena ocupación, la cohesión social y el progreso científico y técnico, de manera que se asegure a toda la ciudadanía el acceso a los servicios públicos y el derecho a la salud, la educación, la vivienda, la protección social, el ocio y la cultura.

De acuerdo con los artículos 30.1 y 31.14 del Estatuto de Autonomía de las Illes Balears, corresponden a la Comunidad Autónoma de las Illes Balears, respectivamente, la competencia exclusiva respecto a la organización, régimen y funcionamiento de las instituciones propias en el marco del Estatuto, el desarrollo legislativo y la ejecución de la protección de datos de carácter personal 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.

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 (de ahora en adelante, RGPD), señala que la protección de los derechos y las libertades de las personas físicas respecto al tratamiento de datos personales exige la adopción por el responsable del tratamiento de medidas técnicas y organizativas apropiadas con objeto de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, entre las que se incluye la regulación de las políticas de protección de datos (artículo 24.2 del RGPD).

En este sentido, el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (de ahora en adelante, LOPDGDD), dispone que los responsables determinarán las medidas técnicas y organizativas apropiadas que deben aplicar para garantizar y acreditar que el tratamiento es conforme con el RGPD, la LOPDGDD, sus normas de desarrollo y la legislación sectorial aplicable.

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13, letra *h)*, sobre derechos de las personas en sus relaciones con las administraciones públicas, el derecho a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que las administraciones públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos. Dichos medios deberán asegurar la interoperabilidad y la seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

En este sentido, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, recogido en el artículo 156 de la Ley 40/2015, de 1 de octubre, establece los principios básicos y los requisitos mínimos necesarios para una protección adecuada de la información tratada y de los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos.

II

La organización de la Administración de la Comunidad Autónoma de las Illes Balears se fundamenta en una estructura jerárquicamente ordenada. Así, bajo la dirección superior de la Presidencia del Gobierno, la Ley 3/2003, de 26 de marzo, de Régimen Jurídico de la Administración de la Comunidad Autónoma de las Illes Balears, establece como órganos superiores a los consejeros, y como órganos directivos a los directores generales, los secretarios generales y aquellos otros que se asimilen a estos en rango. Las consejerías se configuran como los sectores materiales de actividad administrativa funcionalmente homogéneos, cuya creación y estructura orgánica básica corresponde establecer a la Presidencia del Gobierno.

De acuerdo con el artículo 17.*a)* de la Ley 1/2019, de 31 de enero, del Gobierno de las Illes Balears, corresponde al Consejo de Gobierno establecer la política general de la comunidad autónoma, dentro de la cual está la política de protección de datos personales.

En consecuencia, en cumplimiento del artículo 24.2 del RGPD, es necesario que el Gobierno de las Illes Balears apruebe su propia Política de Protección de Datos personales que regule los principios rectores, las obligaciones, la estructura, la organización y las responsabilidades que deberá prever la Administración de la Comunidad Autónoma de las Illes Balears (en adelante, CAIB) en materia de protección de datos personales y derechos digitales.

Así, la Política de Protección de Datos Personales que se aprueba por decreto es aplicable a la Administración de la CAIB, y de aplicación supletoria al sector público instrumental de esta Administración, regulado por la Ley 7/2010, de 21 de julio, del sector público instrumental de la Comunidad Autónoma de las Illes Balears, siempre que el ente en concreto no tenga aprobada su propia política de protección de datos, y sin perjuicio de la adaptación correspondiente a las particularidades propias de cada ente.

III

El principio de «responsabilidad proactiva» (artículo 5.2 del RGPD) requiere que los responsables del tratamiento, es decir, los titulares de los órganos directivos de las consejerías (directores generales y secretarios generales) y órganos directivos asimilados analicen qué datos se tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de estos conocimientos deberán determinar de forma explícita la manera como se aplicarán las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme con el RGPD. Por lo tanto, este principio exige una actitud consciente, diligente y proactiva por parte de los responsables ante todos los tratamientos de datos personales que se lleven a cabo en la Administración de la CAIB.

El documento «maestro» de todo el «*compliance*» son las políticas de protección de datos personales dado que, para poder demostrar la conformidad con el RGPD, el responsable del tratamiento deberá adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

En este sentido, la Política de Protección de Datos personales es el documento base y el marco de gobierno mediante el cual se define el marco de actuación que permite recoger y delimitar con claridad las responsabilidades y funciones en materia de protección de datos personales en el contexto de las actividades de tratamiento de los datos personales y los sistemas de información de la Administración de la CAIB.

Además, la adopción de un marco de gobierno de protección de datos personales permite la colaboración de todos los niveles de la Administración —estratégico, táctico y operativo—, para gestionar los datos personales que se derivan de las actividades de tratamiento de la Administración de la CAIB, fomentando así una cultura de protección de datos en todos los niveles de la Administración autonómica.

IV

El 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, dispone en su artículo 3.2.*b)* que se adscribe a la Secretaría General de la Consejería de Presidencia y Administraciones Públicas, a efectos administrativos, la Delegación de Protección de Datos Personales.

De acuerdo con el artículo 3.6 del citado Decreto, las secretarías generales y las direcciones generales, así como los órganos directivos asimilados, son los responsables del tratamiento de los datos personales en relación con sus competencias.

Asimismo, el artículo 2.1 letra e) del Decreto 12/2023, modificado entre otros por el Decreto 4/2024, de 17 de mayo, de la Presidenta de les Illes Balears, establece que la Dirección General de Estrategia Digital y Simplificación Administrativa tiene las funciones de encargado del

tratamiento de los datos personales en relación con los sistemas de información, recursos tecnológicos y servicios informáticos y telemáticos de la Administración de la Comunidad Autónoma.

V

En consecuencia, se ha considerado necesario dotar a la Administración de la Comunidad Autónoma de las Illes Balears de una estructura organizativa que le permita implementar la Política de Protección de Datos Personales, con la finalidad de llevar a cabo una gestión de las actividades de tratamiento de acuerdo con la normativa vigente en materia de protección de datos personales y derechos digitales mediante la aprobación del Decreto 44/2024, de 4 de otubre, por el que se crea y se regula la estructura organizativa de la protección de datos de la Administración de la Comunidad Autónoma de las Illes Balears.

VI

Por lo tanto, el objeto de este decreto es la aprobación de la Política de Protección de Datos Personales de la Administración de la CAIB para definirla, implantarla y gestionarla. Así, este Decreto cumple los principios de buena regulación exigidos por el artículo 49 de la Ley 1/2019, de 31 de enero, y por el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Este decreto contiene veintidós artículos y una disposición final.

Se han respetado los principios de necesidad, eficacia, proporcionalidad y seguridad jurídica, dado que el Decreto recoge la regulación imprescindible para atender la necesidad que debe cubrirse, y es coherente con el resto del ordenamiento, especialmente en relación con la regulación en materia de protección de datos contenida en el RGPD y en la LOPDGDD, y se ha seguido el procedimiento establecido para la elaboración normativa de disposiciones reglamentarias previsto en la Ley 1/2019, de 31 de enero.

Igualmente, se ha respetado el principio de transparencia, dado que el Proyecto de decreto se ha publicado en el Portal de Transparencia y se ha sometido a información pública, de manera que se ha facilitado la presentación de alegaciones y sugerencias.

Finalmente, se han respetado los principios de eficiencia, calidad y simplificación, dado que el referido Decreto no regula procedimientos que supongan nuevas cargas administrativas a la ciudadanía.

Por todo ello, a propuesta de la consejera de Presidencia y Administraciones Públicas, con el informe preceptivo favorable de la Agencia Española de Protección de Datos, de acuerdo con el Consejo Consultivo de las Illes Balears, y previa deliberación del Consejo de Gobierno en la sesión del día 22 de noviembre de 2024,

DECRETO

Capítulo I
Disposiciones generales

Artículo 1
Objeto

Este decreto tiene por objeto regular la Política de Protección de Datos Personales (de ahora en adelante, PPDP) de la Administración de la Comunidad Autónoma de 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.

Artículo 2
Ámbito de aplicación

1. Este decreto se aplica a todos los sistemas de información y a todas las actividades de tratamiento de datos personales de los que sea responsable o encargada del tratamiento la Administración de la CAIB.

Por lo tanto, la Política de Protección de Datos Personales de la Administración de la CAIB es de obligado cumplimiento para todas las unidades que conforman la estructura de la Administración de la CAIB (direcciones generales, secretarías generales y órganos directivos asimilados) y para todo el personal con acceso a la información de la que es responsable o encargada esta Administración, con independencia de su destino, condición laboral o relación por la que se accede a la información.

2. El Decreto por el que se aprueba la Política de Protección de Datos Personales de la Administración de la CAIB es de aplicación supletoria al sector público instrumental de la CAIB, regulado por la Ley 7/2010, de 21 de julio, del sector público instrumental de la Comunidad

Autónoma de las Illes Balears, sin perjuicio de las debidas adaptaciones a las particularidades organizativas propias de cada ente, y siempre que estos entes no tengan aprobada su propia política de protección de datos.

Artículo 3
Marc normativo

El marco normativo de aplicación del Decreto por el que se aprueba la Política de Protección de Datos Personales de la Administración de la CAIB está integrado por 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 con respecto al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y demás normativa vigente de aplicación en materia de protección de datos personales y derechos digitales.

Capítulo II
Principios de protección de datos

Artículo 4
Principios relativos al tratamiento de datos personales

1. La Administración de la Comunidad Autónoma de las Islas Baleares debe tratar la información y los datos de carácter personal, bajo su responsabilidad, de acuerdo con los principios de protección de datos regulados en el artículo 5 del Reglamento (UE) 2016/679.

2. Los titulares de los órganos directivos de las Consejerías de la Administración de la Comunidad Autónoma de las Illes Balears (Directores generales, Secretarios generales y órganos directivos asimilados) como responsables del tratamiento, deben adoptar las medidas técnicas y organizativas apropiadas por para garantizar y poder demostrar ante los interesados y la autoridad de control (Agencia Española de Protección de Datos), que el tratamiento es conforme con el Reglamento (UE) 2016/679, de acuerdo con el principio de «responsabilidad proactiva».

3. De acuerdo con el «principio de licitud», 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).

Ahora bien, la base jurídica de cada tratamiento concreto deberá especificarse en la norma o acto jurídico que, en cada caso, establezca el tratamiento en sí mismo considerado, y deberá reflejarse en el Registro de Actividades de Tratamiento (RAT) y publicarse en el Inventario de las actividades de tratamiento.

4. El RGPD ha desplazado el «principio de consentimiento» como eje central del derecho a la protección de datos en el ámbito de las administraciones públicas, por lo que el consentimiento como base jurídica del tratamiento de datos personales por las Administraciones Públicas tiene carácter excepcional.

Así, el consentimiento no puede constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal cuando exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando este responsable es una autoridad pública y sea, por tanto, improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular.

5. Los responsables del tratamiento deben tomar las medidas oportunas para facilitar al interesado, a título gratuito, toda la información recogida en los artículos 13 y 14 del RGPD, así como cualquier comunicación de acuerdo con los artículos 15 a 22 y 34 del RGPD relativa al tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, acorde con el «principio de transparencia».

6. Los datos de carácter personal deben tratarse para el cumplimiento de finalidades determinadas, explícitas y legítimas en el momento de la recogida, y no pueden ser tratados posteriormente de forma incompatible con estas finalidades, de acuerdo con el «principio de limitación de la finalidad». La finalidad del tratamiento deberá quedar determinada en la base jurídica que legitime el tratamiento.

7. Para aplicar el «principio de minimización de datos» el responsable del tratamiento debe aplicar las medidas técnicas y organizativas apropiadas que garanticen que, por defecto, únicamente sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento y que hayan sido definidos en la etapa de diseño inicial.

No se pueden solicitar y tratar datos personales simplemente por si pudieran resultar útiles o «para tenerlos».

8. De acuerdo con el «principio de exactitud» en un tratamiento que incorpora un sistema de Inteligencia Artificial (IA) es necesario evaluar la exactitud de los datos de entrada, los datos de salida e incluso los datos intermedios, dado que no hacerlo podría introducir sesgos y comprometer el rendimiento no sólo del algoritmo sino de todo el tratamiento.

Los tratamientos que incorporen o utilicen un sistema de IA deberán cumplir, con carácter específico, aparte de los requisitos para la protección de datos personales que resulten del RGPD y de la 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 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).

Los responsables del tratamiento deben adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan, a fin de que éstos sean exactos y, si fuera necesario, actualizados.

9. El «principio de limitación del plazo de conservación» constituye una de las materializaciones del «principio de minimización». La conservación de estos datos debe limitarse en el tiempo a conseguir las finalidades que persigue el tratamiento. Una vez alcanzadas estas finalidades, según corresponda conforme a los artículos 22, 32 o concordantes de la LOPDGDD, los datos deben ser eliminados, bloqueados o, en su defecto, anonimizados, es decir, desprovistos de todo elemento que permita identificar a los interesados.

10. Los datos personales se tratarán de forma que se garantice una seguridad y confidencialidad adecuadas de los datos personales, incluso para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

Los responsables del tratamiento deben aplicar las medidas técnicas y/u organizativas apropiadas y necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de la información, y una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, a fin de proteger los derechos y libertades de las personas, de acuerdo con el «principio de integridad y confidencialidad».

Deben evitarse los tratamientos de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo.

Artículo 5
Consentimiento de los menores de edad

1. El tratamiento de los datos personales de un menor de edad solo se puede fundar en el consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para celebrar el acto o el negocio jurídico en cuyo contexto se solicite el consentimiento para el tratamiento.

2. El tratamiento de los datos personales de los menores de catorce años, fundamentado en el consentimiento, solo es lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 6
Exclusiones

1. El Reglamento (UE) 2016/679 no se aplica al tratamiento de la información anónima, incluso con fines estadísticos o de investigación, sin perjuicio de que sí será de aplicación al propio tratamiento de datos personales conducente a su anonimización.

Los principios de protección de datos no se aplican a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.

2. El Reglamento (UE) 2016/679 no se aplica a la protección de datos personales de personas fallecidas.

Ahora bien, las personas vinculadas a la persona difunta por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento con objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión, excepto cuando la persona difunta lo haya prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

3. El RGPD no se aplica al tratamiento de datos de carácter personal por una persona física en el ejercicio de actividades exclusivamente

personales o domésticas.

4. El RGPD no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

Capítulo III
Derechos de los interesados

Artículo 7
Ejercicio de los derechos de los afectados

1. Los interesados pueden ejercer ante los responsables de cada tratamiento (según el caso, los titulares de los órganos directivos o de los órganos directivos asimilados de las consejerías de la CAIB), los derechos de información, acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y de no ser objeto de decisiones individuales automatizadas, derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

2. Los responsables del tratamiento deben adoptar las medidas adecuadas en cada uno de los órganos directivos de la Administración de la CAIB para garantizar a los afectados el ejercicio de sus derechos.

Sin perjuicio del derecho de los interesados de relacionarse, cuando corresponda, con las Administraciones Públicas a través de medios no electrónicos (art. 14 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas), en la sede electrónica de la Administración de la CAIB *(https://www.caib.es/seucaib/es/200/persones/tramites/tramite/3960058)* están habilitados los procedimientos para el ejercicio de los derechos en materia de protección de datos personales por los interesados en el ámbito de la Administración de la CAIB.

3. Los responsables del tratamiento deben atender las solicitudes de ejercicio de los derechos de acuerdo con los artículos 15 a 22 del RGPD, sin dilación indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud.

Dicho plazo puede prorrogarse dos meses más en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. 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.

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 la Agencia Española de Protección de Datos y de ejercitar acciones judiciales.

La prueba del cumplimiento del deber de responder a las solicitudes de ejercicio de los derechos formulados por los afectados recaerá sobre el responsable del tratamiento.

4. Los Coordinadores de protección de datos personales colaborarán con los responsables del tratamiento en la atención y tramitación de las solicitudes de ejercicio de derechos de los interesados, así como en la tramitación y resolución de las reclamaciones presentadas por los afectados ante la Agencia Española de Protección de Datos, sin perjuicio del asesoramiento en su caso del Delegado de Protección de Datos de la Administración de la CAIB.

5. La información facilitada en virtud de los artículos 13 y 14 del RGPD así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 del RGPD serán a título gratuito.

Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento puede cobrar una tasa en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o negarse a actuar respecto de la solicitud.

A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se puede considerar repetitivo el ejercicio del derecho de acceso más de una vez durante el plazo de seis meses, salvo que exista causa legítima.

6. El derecho de acceso del artículo 15 del RGPD es independiente del derecho de acceso a la información pública que regula la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

También es independiente del derecho de acceso a la documentación en un procedimiento administrativo, regulado por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

7. De acuerdo con el artículo 12.5 de la LOPDGDD, cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial para el ejercicio de los derechos del Reglamento (UE) 2016/679 se aplicarán las leyes especiales.

8. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

Capítulo IV
Responsable y encargado del tratamiento

Artículo 8
Responsable del tratamiento

1. Los titulares de los órganos directivos de las consejerías de la CAIB y los órganos directivos asimilados, dado que determinan las finalidades y los medios de los tratamientos, son los responsables de los tratamientos de los datos personales de la Administración de la CAIB.

2. El artículo 3.6 del 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, dispone que las secretarías generales y las direcciones generales, así como los órganos directivos asimilados, ejercen las funciones de responsables del tratamiento de los datos personales de los procedimientos o procesos en relación con sus competencias.

Actualmente, de acuerdo con la normativa vigente, los órganos directivos de las consejerías de la Administración de la CAIB son los directores generales, los secretarios generales y los secretarios autonómicos, y los órganos directivos asimilados.

Estos últimos son actualmente la directora de la Oficina Balear de la Infancia y la Adolescencia (OBIA), el interventor general de la Comunidad Autónoma de las Illes Balears y los directores territoriales de Educación de Menorca y de Ibiza y Formentera.

3. Los secretarios generales, directores generales y secretarios autonómicos de las consejerías de la CAIB, la directora de la Oficina Balear de la Infancia y la Adolescencia (OBIA), el interventor general de la Comunidad Autónoma de las Illes Balears y los directores territoriales de Educación de Menorca y de Ibiza y Formentera deben disponer de un buzón electrónico corporativo para atender, como responsables del tratamiento, todas las cuestiones relativas al tratamiento de los datos personales y, específicamente, las solicitudes de ejercicio de los derechos de los interesados.

Esta dirección electrónica debe tener el siguiente formato *responsabledades@*, seguido del dominio correspondiente al órgano directivo, por ejemplo *responsabledades@sgcpres.caib.es* en el supuesto de la Secretaría General de la Consejería de Presidencia y Administraciones Públicas, y debe estar visible en la Sede Electrónica de la CAIB y en el portal del Gobierno de las Illes Balears.

A esta dirección electrónica deben tener acceso los coordinadores de protección de datos respectivos de cada una de las consejerías para asistir a los responsables del tratamiento.

4. Por otro lado, cuando dos o más responsables determinen conjuntamente las finalidades y los medios del tratamiento serán considerados corresponsables del tratamiento.

Los corresponsables deben determinar de manera transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD, en particular con respecto al ejercicio de los derechos de la persona interesada y las obligaciones de suministro de información respectivas de los artículos 13 y 14 del RGPD.

Independientemente de los términos del acuerdo, los interesados pueden ejercer sus derechos ante, y en contra de, cada uno de los responsables.

5. Los responsables del tratamiento, en el ámbito de sus competencias, ejercen las siguientes funciones específicas:

a) Implantar la Política de Protección de Datos Personales de la Administración de la CAIB.
b) Velar por el cumplimiento efectivo del RGPD, la LOPDGDD, la PPD y la normativa vigente de protección de datos personales y derechos digitales.
c) Mantener, actualizar y llevar la gestión del registro de las actividades de tratamiento de datos personales (RAT) en el ámbito de sus competencias.
d) Acordar, aplicar, revisar y actualizar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluya, entre otros, la seudonimización, el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, la capacidad de restaurar la disponibilidad y el

acceso a los datos personales de manera rápida en caso de incidente físico o técnico, y un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

e) Garantizar que, por defecto, únicamente se tratan los datos personales necesarios para cada una de las finalidades específicas del tratamiento y, en particular, que los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. Esta obligación se aplica a la cantidad de datos personales recogidos, al alcance del tratamiento, al plazo de conservación y a la accesibilidad de los datos.

f) Garantizar el cumplimiento de las obligaciones de secreto y confidencialidad derivadas de la normativa en materia de protección de datos personales con respecto a los tratamientos que gestionan.

g) Garantizar el cumplimiento de la obligación de informar adecuadamente a los interesados y aplicar el principio de transparencia en la recogida de los datos personales.

h) Garantizar el ejercicio de los derechos de los interesados, de acuerdo con los artículos 15 a 22 del RGPD.

i) Elegir, cuando se realice un tratamiento por cuenta de un responsable, únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos de los interesados.

j) Evaluar el impacto de las operaciones de tratamiento en la protección de datos personales (EIPD) antes del tratamiento, cuando sea probable que un tipo de tratamiento pueda entrañar un alto riesgo para los derechos y las libertades de las personas físicas.

k) Notificar, en tiempo y forma, las violaciones de seguridad de los datos personales a la Agencia Española de Protección de Datos (autoridad de control competente) de acuerdo con el artículo 33 del RGPD, y llevar a cabo su gestión en coordinación con la Dirección General de Estrategia Digital y Simplificación Administrativa de la Consejería de Economía, Hacienda e Innovación.

l) Comunicar la violación de la seguridad de los datos personales a los interesados, sin dilación indebida, cuando sea probable que dicha violación entrañe un alto riesgo para los derechos y las libertades de las personas físicas, de acuerdo con el artículo 34 del RGPD.

m) Asistir a las sesiones y participar activamente en el correspondiente Comité de responsables de la respectiva consejería.

n) Impulsar, fomentar y promover recursos y medios para la concienciación y formación del personal de la Administración de la CAIB en materia de protección de datos de carácter personal.

o) Garantizar que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, y facilitar el acceso a los datos personales y a las operaciones de tratamiento.

p) Atender las recomendaciones, sugerencias y observaciones de la Delegación de Protección de Datos de la Administración de la CAIB.

q) Respaldar al delegado de protección de datos en el ejercicio de sus funciones, facilitándole los recursos necesarios para el ejercicio de dichas funciones y para el mantenimiento de sus conocimientos especializados.

r) Las demás funciones y competencias que les atribuye la legislación aplicable en materia de protección de datos personales y derechos digitales.

6. Los responsables del tratamiento están sujetos al deber de confidencialidad del artículo 5.1.f) del RGPD.

Esta obligación será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

Ambas obligaciones se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable del tratamiento.

Artículo 9
Encargado del tratamiento

1. El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata los datos personales por cuenta del responsable del tratamiento, de acuerdo con el artículo 4. 8) del RGPD.

Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado.

2. El tratamiento de los datos personales por el encargado de tratamiento se debe regir por un contrato o por otro acto jurídico, de acuerdo con el artículo 28 del RGPD, que vincule al encargado respecto del responsable del tratamiento y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Dicho contrato o acto jurídico recogerá las circunstancias del art. 28.3 del RGPD, y en particular, deben adoptarse y documentarse en este contrato o acto jurídico las medidas que garanticen que el encargado del tratamiento ofrece garantías suficientes para el cumplimiento de la normativa de protección de datos.

3. Cuando el órgano de contratación no coincida con el responsable del tratamiento se debe suscribir un contrato independiente al contrato principal (vinculado a este) entre el responsable del tratamiento y el encargado (adjudicatario del contrato), que recoja todas las condiciones

del artículo 28.3 del RGPD.

Asimismo, 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 del artículo 122.2 letras a) a e) de la LCSP recogidas en dicho precepto (que además tienen la consideración de esenciales a los efectos del artículo 211.1.f) de la LCSP).

4. El encargado de tratamiento debe ejercer las funciones y competencias que se determinen en este contrato que, como mínimo, deben ser las previstas en el artículo 28 del RGPD y la normativa en vigor en materia de protección de datos de carácter personal.

5. Para el caso de que la contratación pública implique el acceso del contratista a datos de carácter personal de los que sea responsable la Administración de la CAIB, aquel tendrá la consideración de encargado del tratamiento, de acuerdo con el artículo 28 del RGPD en relación con la disposición adicional vigésima quinta de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

6. Cuando haya solicitudes de ejercicio de los derechos, el encargado debe asistir al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

7. El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

8. Los encargados del tratamiento están sujetos al deber de confidencialidad del artículo 5.1.f) del RGPD.

Esta obligación será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

Ambas obligaciones se mantendrán aun cuando hubiese finalizado la relación del obligado con el encargado del tratamiento.

9. Si un encargado del tratamiento infringe el RGPD al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento, de acuerdo con el artículo 28.10 del RGPD.

Capítulo V
Medidas de responsabilidad proactiva

Artículo 10
Protección de datos desde el diseño y por defecto

1. Protección de datos desde el diseño

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.

2. Protección de datos por defecto

Los responsables de los tratamientos deben aplicar las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, únicamente se tratan los datos personales necesarios para cada uno de los fines específicos del tratamiento.

Esta obligación se aplica a la cantidad de datos personales recogidos, al alcance del tratamiento, al plazo de conservación y a la accesibilidad de los datos. Estas medidas deberán garantizar en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

4. La seudonimización implica que el tratamiento de datos personales ya no pueda atribuirse a una persona interesada sin utilizar información adicional, siempre que esta información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Artículo 11
Registro de actividades de tratamiento (RAT)

1. Los titulares de los órganos directivos de las consejerías de la CAIB y los órganos directivos asimilados, como responsables del tratamiento, deben llevar y mantener un registro de las actividades de tratamiento (en adelante, RAT) efectuadas bajo su responsabilidad que debe contener toda la información del artículo 30 del RGPD.

2. La Administración de la CAIB debe publicar en el Portal de Transparencia del Gobierno de las Illes Balears el Inventario de las actividades de tratamiento de los responsables del tratamiento, accesible por medios electrónicos, en el que debe constar la información del artículo 30 del RGPD y su base legal (artículo 31.2 de la LOPDGDD).

3. Los responsables del tratamiento de la Administración de la CAIB deben utilizar la última versión de la herramienta GESTIONA_RGPD de la Agencia Española de Protección de Datos (AEPD) para la gestión del RAT y la generación del Inventario de tratamientos.

Esta herramienta de ayuda y apoyo a la decisión de los responsables permite también la generación de las bases mínimas para iniciar las actividades de análisis y gestión de riesgos en el ámbito del RGPD, la generación de informes en formato DOC, HTML y CSV para facilitar su exportación y uso en otras herramientas, y la gestión y almacenamiento local de los datos.

La gestión del tratamiento se realiza en el propio navegador del usuario, sin que se transmitan datos a la AEPD y con total confidencialidad.

4. Los coordinadores de protección de datos personales deben apoyar a los responsables del tratamiento y colaborar con éstos en la gestión y el mantenimiento del RAT y del Inventario de tratamientos, sin perjuicio de la supervisión y el asesoramiento de la Delegación de Protección de Datos de la Administración de la CAIB.

5. El RAT y la publicación del Inventario de tratamientos deben estar permanentemente actualizados, y las modificaciones deben comunicarse a la Delegación de Protección de Datos de la Administración de la CAIB antes de que el cambio se haya reflejado tanto en el RAT como en la publicación del Inventario.

6. Cada encargado del tratamiento de la Administración de la CAIB llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga toda la información del artículo 30.2 del RGPD.

7. Los responsables y encargados del tratamiento están obligados a cooperar con la Agencia Española de Protección de Datos, y a poner a su disposición, previa solicitud, el RAT, de modo que pueda servir para supervisar las operaciones de tratamiento.

Artículo 12
Análisis de riesgos

1. Los responsables del tratamiento deben evaluar los riesgos inherentes a los tratamientos y aplicar las medidas para mitigarlos, como el cifrado, de forma que puedan garantizar, tanto como estar en condiciones de demostrar, que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGDD.

La gestión del riesgo requiere una gestión proactiva por parte de los responsables del tratamiento. El riesgo surge tanto por el tratamiento automatizado de datos como por el procesamiento manual, por los elementos humanos y por los recursos implicados.

2. Todos los tratamientos de datos personales requieren un análisis de riesgos que se llevará a cabo de forma periódica y, en cualquier caso, siempre que haya un cambio significativo en los sistemas de información o en los tratamientos de datos personales, con la finalidad de identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables.

La actualización del análisis de riesgos no sólo procederá cuando se produzca una modificación del tratamiento, sino también, cuando haya un cambio de contexto, por ejemplo, cuando haya algún tipo de amenaza por la aparición de un nuevo virus o ataque informático, o cuando exista un nuevo contexto, político, social o económico que suponga un aumento del riesgo.

En cumplimiento del principio de responsabilidad proactiva o *accountability*, la gestión del riesgo debe estar documentada.

3. Las medidas de seguridad garantizarán la preservación de la confidencialidad, la integridad y la disponibilidad de la información, la autenticidad, la responsabilidad y la fiabilidad, 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.

4. En caso de encargos de tratamiento, el encargado del tratamiento tiene la obligación de asistir al responsable del tratamiento a la hora de realizar la gestión del riesgo, dentro de los límites del objeto del encargo.

Artículo 13
Evaluación de impacto de protección de datos (EIPD)

1. Los directores generales, secretarios generales y órganos directivos asimilados de la Administración de la CAIB realizarán, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento (EIPD) en la protección de datos personales, cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, de acuerdo con el artículo 35 del RGPD.

2. Los coordinadores de protección de datos personales colaborarán con los responsables del tratamiento en la realización y seguimiento de las evaluaciones de impacto de las operaciones de tratamiento (EIPD), sin perjuicio del asesoramiento del Delegado de Protección de Datos de la Administración de la CAIB, como órgano independiente.

3. Los responsables examinarán si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo en las operaciones de tratamiento.

Una única evaluación puede abordar una serie de operaciones de tratamiento similares que comporten altos riesgos similares.

4. Serán objeto de consulta previa a la AEPD las evaluaciones de impacto relativas a la protección de datos (EIPD) de aquellos tratamientos que, cumpliendo con los principios y derechos establecidos en el RGPD, sean de alto riesgo para los derechos y libertades de los interesados, y cuando el responsable no haya podido mitigar o evitar dicho riesgo.

Para realizar una solicitud de consulta previa de la EIPD a la AEPD, entre el contenido mínimo exigido por el artículo 36.3 del RGPD, hay que tener en cuenta que el desarrollo de la documentación de la EIPD debe contemplar lo señalado por la AEPD en sus guías y recomendaciones, en particular, lo señalado en la guía «Gestión del riesgo y evaluación de impacto en tratamientos de datos personales» disponible en la web de la AEPD, de acuerdo con la Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos.

5. El tratamiento de datos personales sin haber realizado antes del tratamiento la EIPD, en los supuestos en que ésta sea exigible:

a) Debe suspenderse, realizarse la EIPD y su valoración antes de reanudar el tratamiento.
b) Es una infracción grave del artículo 73, letra t), de la LOPDGDD.

Artículo 14
Violaciones o brechas de seguridad de los datos de carácter personal

1. La violación o brecha de seguridad de los datos de carácter personal es un incidente de seguridad que ocasiona la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otro modo, o la comunicación o acceso no autorizados a estos datos.

Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden implicar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como por ejemplo pérdida de control sobre los datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de la confidencialidad de los datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión.

2. Los directores generales, secretarios generales y órganos directivos asimilados de la Administración de la CAIB, en caso de producirse una brecha de seguridad, la notificarán a la Agencia Española de Protección de Datos (AEPD) a través del procedimiento de notificación de brechas de seguridad de la Sede Electrónica de la AEPD, sin dilación indebida y, de ser posible, en un plazo máximo de 72 horas después de que hayan tenido constancia de ella, salvo que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas, de conformidad con el artículo 33 del RGPD.

Si la notificación a la AEPD no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

3. Los coordinadores de protección de datos personales de las consejerías de la Administración de la CAIB colaborarán con los responsables del tratamiento en la tramitación y resolución de las brechas de seguridad, sin perjuicio del asesoramiento del Delegado de Protección de Datos de la Administración de la CAIB, como órgano independiente, y del responsable de seguridad de la Información de la Dirección General de Estrategia Digital y Simplificación Administrativa.

4. La Dirección General de Estrategia Digital y Simplificación Administrativa de la Consejería de Economía, Hacienda e Innovación debe notificar las brechas de seguridad de los datos personales al Centro Criptológico Nacional (CCN-CERT) a través de la herramienta LUCIA, herramienta desarrollada por el CCN-CERT para la gestión y notificación de ciberincidentes de las entidades dentro del ámbito de aplicación del Esquema Nacional de Seguridad.

5. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida, en un lenguaje claro y sencillo, de acuerdo con el artículo 34 del RGPD.

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones señaladas en las letras a) a c) del artículo 34.3 del RGPD.

Capítulo VI
Estructura organizativa de la protección de datos

Artículo 15
Estructura organizativa en la Administración de la CAIB

El Decreto 44/2024, de 4 de octubre, por el que se crea y regula la estructura organizativa de la protección de datos de la Administración de la Comunidad Autónoma de las Illes Balears, a fin de implementar la Política de Protección de Datos Personales, establece la siguiente estructura organizativa:

1. Comisión de Protección de Datos (de ahora en adelante, CPD)
2. Comité Técnico de Coordinadores de Protección de Datos Personales
3. Comité de responsables del tratamiento para cada una de las consejerías
4. Coordinadores de protección de datos personales de las consejerías

Artículo 16
Delegación de Protección de Datos de la Administración de la CAIB

1. La Delegación de Protección de Datos de la Administración de la CAIB se adscribe administrativamente a la Secretaría General de la Consejería de Presidencia y Administraciones Públicas, de acuerdo con el artículo 3.2.*b)* del 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.

La Delegación de Protección de Datos de la Administración de la CAIB atiende las competencias en materia de protección de datos personales de la Administración de la CAIB, integrada por las diferentes consejerías, en aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. La Delegación de Protección de Datos de la Administración de la CAIB no incluye a los entes del sector público instrumental de la CAIB y, en consecuencia, no tiene competencias sobre estos entes, regulados por la Ley 7/2010, de 21 de julio, del sector público instrumental de la Comunidad Autónoma de las Illes Balears, los cuales deben tener su propio delegado de protección de datos.

Tampoco están incluidos en el ámbito de las competencias de la Delegación de Protección de Datos de la Administración de la CAIB los centros docentes públicos no universitarios de las Illes Balears, los cuales disponen de su propio delegado de protección de datos, de acuerdo con el artículo 34.1.*b)* de la LOPDGDD.

3. La Delegación de Protección de Datos de la Administración de la CAIB tiene su sede en la Consejería de Presidencia y Administraciones Públicas (paseo de Sagrera, 2, 07012 Palma), y dispone del buzón de correo electrónico corporativo *protecciodades@dpd.caib.es* para atender las cuestiones relativas al tratamiento de los datos personales y al ejercicio de los derechos de los interesados, de acuerdo con el artículo 38.4 del RGPD.

4. El organigrama de la Delegación de Protección de Datos de la Administración de la CAIB se desarrollará mediante un decreto que regulará la estructura organizativa de la Delegación de Protección de Datos, de acuerdo con los artículos 37 a 39 del RGPD y 34 a 37 de la LOPDGDD.

Ésta podrá contar, para un mejor desarrollo de sus funciones, con el apoyo de subdelegaciones especializadas en los diferentes ámbitos orgánicos de la Administración de la CAIB.

5. La consejería que tenga adscrita la Delegación de Protección de Datos de la Administración de la CAIB debe garantizar que ésta disponga de los recursos humanos y materiales necesarios para el ejercicio de sus funciones.

6. La persona titular de la Delegación de Protección de Datos de la Administración de la CAIB, el Delegado de Protección de Datos (de ahora en adelante, DPD), ejerce las funciones del artículo 39 del RGPD con plena autonomía e independencia funcional en los términos

establecidos en el Reglamento (UE) 2016/679. El DPD rendirá cuentas directamente al más alto nivel jerárquico del responsable del tratamiento.

El delegado de protección de datos no será destituido ni sancionado por el responsable o el encargado del tratamiento por desempeñar sus funciones. La Administración de la CAIB garantizará la independencia del DPD, evitando cualquier conflicto de intereses.

7. Con respecto a la cualificación del Delegado de Protección de Datos de la Administración de la CAIB, el cumplimiento de los requisitos del artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos se acreditará a través de mecanismos de certificación de acuerdo con las exigencias del Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD).

8. La Administración de la CAIB y los responsables del tratamiento:

a) Garantizarán que el delegado de protección de datos participa de manera adecuada y en el momento oportuno en todas las cuestiones relativas a la protección de datos personales.
b) Apoyarán al delegado de protección de datos en el desempeño de las funciones del artículo 39 del RGPD.
c) Facilitarán los recursos necesarios para cumplir sus tareas y para acceder a los datos personales y a las operaciones de tratamiento, así como para mantener su conocimiento especializado.
d) Garantizarán que el delegado de protección de datos no recibe ninguna instrucción con respecto al ejercicio de sus funciones.

9. El delegado de protección de datos, en el ejercicio de sus funciones de asesoramiento y supervisión dirigidas a garantizar el cumplimiento de la normativa de protección de datos personales:

a) Puede inspeccionar los procedimientos relacionados con el objeto de la LOPDGDD y emitir recomendaciones en el ámbito de sus competencias.
b) Debe tener acceso a los datos personales y procesos de tratamiento, y los responsables o los encargados del tratamiento no pueden oponer a este acceso la existencia de cualquier deber de confidencialidad o secreto, incluyendo lo previsto en el artículo 5 de la LOPDGDD.
c) Cuando aprecie la existencia de una vulneración relevante en materia de protección de datos, la documentará y comunicará inmediatamente al responsable o al encargado del tratamiento.

Artículo 17
Centros docentes públicos no universitarios de las Illes Balears

1. Delegado de protección de datos

Los centros docentes públicos no universitarios de las Illes Balears de régimen ordinario y de régimen especial, de acuerdo con el artículo 34.1.*b)* de la LOPDGDD, tienen designado actualmente un único delegado de protección de datos.

Dada la complejidad estructural de los centros docentes públicos no universitarios de las Illes Balears de régimen ordinario y de régimen especial, regulados estos últimos en el capítulo VII y el artículo 107 de la Ley 1/2022, de 8 de marzo, de Educación de las Illes Balears, y que incluyen, entre otros, las «escuelas oficiales de idiomas» (EOI) y los «conservatorios profesionales de música y danza» (CMD), se podrán designar otros delegados de protección de datos para atender las especialidades propias de los centros de régimen especial.

Los datos de contacto del DPD de los centros docentes públicos no universitarios de las Illes Balears es *dpdcentreseducatiuspublics@sgtedu.caib.es*.

2. Responsables del tratamiento en la comunidad educativa

2.1. La persona titular de la dirección de cada centro docente público no universitario de las Illes Balears es la responsable del tratamiento respecto de los tratamientos de datos personales específicos de su centro educativo, de los cuales determina los fines y medios del tratamiento.

2.2. En los tratamientos transversales de todos los centros docentes públicos no universitarios de las Illes Balears los responsables del tratamiento son, en función de cada una de sus competencias, los directores generales de cada área educativa de la Consejería competente en materia de Educación.

3. Coordinador de bienestar y protección

Los centros docentes públicos no universitarios de las Illes Balears tienen nombrados a sus coordinadores de bienestar y protección del alumnado, que actúan bajo la supervisión de la persona que ejerce la dirección o titularidad del centro, de acuerdo con el artículo 35 de la Ley orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia.

La administración educativa competente deberá establecer los requisitos y las funciones que deben ejercer los coordinadores de bienestar y protección del alumnado, que serán como mínimo los señalados en el artículo 35.2 de la Ley orgánica 8/2021.

Artículo 18
Obligaciones del personal de la CAIB

1. Todo el personal, los órganos y las unidades de la Administración de la CAIB tienen la obligación de conocer y cumplir la PPD, así como las normas y los procedimientos que la desarrollen, prestando su colaboración en las actuaciones de implantación de la Política de Protección de Datos.

2. Todo el personal que presta servicios en la Administración de la CAIB tiene el deber de colaborar en el seguimiento y actualización de las medidas y actuaciones relativas a los tratamientos de datos personales, con el fin de evitar y minorar los riesgos a los que se encuentra expuesto el tratamiento de los datos personales de los que es titular la Administración de la CAIB.

A tal efecto, deben comunicar a los coordinadores de protección de datos de las consejerías, quienes lo comunicarán a los responsables del tratamiento, cualquier propuesta de mejora o sugerencia que ayude a preservar la confidencialidad, la integridad y la disponibilidad de la información y de los datos personales.

3. Deber de confidencialidad

Todas las personas que intervengan en cualquier fase del tratamiento de datos personales están sujetas al deber de confidencialidad a que hace referencia el artículo 5.1.*f)* del RGPD y el artículo 5.1 de la LOPDGDD.

Esta obligación es complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

Ambas obligaciones se mantendrán aunque haya finalizado la relación del obligado con el responsable o encargado del tratamiento.

Capítulo VII
Obligaciones específicas en materia de protección de datos

Artículo 19
Proyectos normativos que implican tratamientos de datos personales

1. Evaluación de impacto (EIPD) en la MAIN

1.1. Los proyectos normativos que impliquen tratamientos de datos personales están sujetos a una evaluación de impacto (EIPD) previa en el marco de la elaboración de la memoria de análisis de impacto normativo (MAIN), de acuerdo con el artículo 35 del RGPD.

La evaluación de impacto de la norma deberá analizar el impacto que tendrá sobre los derechos y las libertades fundamentales de las personas, aportando salvaguardas organizativas, jurídicas y técnicas. Para ayudar a la identificación de los riesgos para los derechos y libertades se recomiendan las herramientas, guías y materiales de la AEPD.

1.2. Aquellas iniciativas que impliquen tratamientos en que intervengan inteligencia artificial, decisiones automatizadas, biometría, vigilancia masiva, centralización a gran escala, tratamiento masivo de datos, datos de menores, de personas vulnerables, etc., deberán tenerse especialmente en cuenta en la evaluación de impacto por implicar riesgos adicionales.

2. Actos administrativos, y disposiciones generales que regulan procedimientos administrativos, en los que hay tratamientos de datos de carácter personal:

Los actos administrativos y disposiciones generales que regulan procedimientos administrativos, que impliquen tratamiento de datos personales deben contemplar todos los requerimientos que les sea de aplicación en materia de protección de datos de carácter personal que se establecen en el RGPD y en la LOPDGDD.

Artículo 20
Concienciación y formación

1. La Administración de la CAIB, junto con los responsables del tratamiento, desarrollará planes y programas de formación continua con la colaboración de la Escuela Balear de Administración Pública (EBAP), así como actividades formativas específicas orientadas a la concienciación y formación del personal que presta sus servicios en la Administración de la CAIB en materia de protección de datos de

carácter personal y derechos digitales, así como a la difusión entre estos del Decreto por el que se aprueba la política de protección de datos, y su desarrollo normativo.

2. La Administración de la CAIB dispondrá de los medios necesarios para que el personal que intervenga en el tratamiento de datos personales sea informado y formado sobre sus deberes y obligaciones en relación con el RGPD y la LOPDGDD, así como de los riesgos existentes en el tratamiento de los datos personales.

3. El Delegado de Protección de Datos de la Administración de la CAIB podrá colaborar en las acciones de concienciación y formación del personal que participa en las operaciones de tratamiento de datos personales, de acuerdo con el artículo 39.1.*b)* del RGPD.

4. El EBAP facilitará al personal, de conformidad con los planes y programas anuales, la formación continua necesaria en materia de protección de datos personales y derechos digitales para desarrollar las competencias que permitan ejercer la prestación de servicios en la modalidad de teletrabajo no presencial.

Artículo 21
Portal web del Gobierno de las Illes Balears y Sede Electrónica

1. El Gobierno de las Illes Balears dispone de dos portales web de protección de datos personales:

a) El portal web de Intranet se ha diseñado como un portal didáctico, informativo, formativo y de ayuda al personal de la Administración de la CAIB, con el fin de poner a su disposición los materiales, herramientas, recursos, guías e información en materia de protección de datos personales necesarios para el ejercicio de sus funciones en relación con el cumplimiento del RGPD y de la LOPDGDD.
b) Con respecto a la ciudadanía, se ha habilitado en Internet un portal web de protección de datos personales para ofrecer un servicio público de información claro, sencillo e intuitivo, a fin de que el ciudadano pueda conocer y ejercer sus derechos en materia de protección de datos personales de acuerdo con el RGPD.

2. Dentro de cada portal web (Intranet e Internet) se ha habilitado un enlace a la Sede Electrónica del Gobierno de las Illes Balears de acceso a los procedimientos para el ejercicio de los derechos de los interesados en materia de protección de datos personales de la Administración de la CAIB.

Estos portales deberán mantenerse actualizados en todo momento, así como la Sede Electrónica, con la colaboración de la Dirección General de Estrategia Digital y Simplificación Administrativa de la Consejería de Economía, Hacienda e Innovación.

Artículo 22
Relación con otras políticas de la Administración de la CAIB

Esta Política de Protección de Datos debe alinearse con los objetivos establecidos en otras políticas de la Administración de la Comunidad Autónoma de las Illes Balears, tales como:

1. Política de gestión documental del Gobierno de las Illes Balears, derivada de la siguiente normativa:

- La Ley 6/2022, de 5 de agosto, de archivos y gestión documental de las Illes Balears.
- El Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- La política de gestión documental del Gobierno de las Illes Balears, aprobada por el Acuerdo del Consejo de Gobierno de 9 de diciembre de 2016 (BOIB n.º 155, de 10 de diciembre).

2. Política de transparencia, derivada de la siguiente normativa:

- La Ley 19/2013, del 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- La Ley 4/2011, de 31 de marzo, de la buena administración y del buen gobierno de las Illes Balears.
- La Ley 37/2007, del 16 de noviembre, sobre reutilización de la información del sector público.
- El Decreto 31/2023, de 22 de mayo, por el cual se establece la organización administrativa en materia de transparencia y se desarrolla el ejercicio del derecho de acceso a la información pública en la Administración de la Comunidad Autónoma de las Illes Balears y en su sector público instrumental.

3. Política de seguridad, derivada de la siguiente normativa:

- El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- La Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma técnica de interoperabilidad de protocolos de intermediación de datos.
- La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), complementa las garantías del Reglamento general de protección de datos (RGPD) en relación con los servicios de la sociedad de la información.

Disposición final única
Entrada en vigor

Este decreto entrará en vigor el día siguiente al de su publicación en el *Boletín Oficial de las Illes Balears*.

Palma, 22 de noviembre de 2024

La presidenta
Margarita Prohens Rigo

La consejera de Presidencia y Administraciones Públicas
Antonia María Estarellas Torrens