Resolución de la Autoridad Portuaria de Gijón por la que se hace público la aprobación de la política de protección de datos personales de la Autoridad Portuaria de Gijón

El Consejo de Administración de la Autoridad Portuaria de Gijón en su sesión de 14 de agosto de 2026, al amparo de lo previsto en el artículo 30.5 letras a) y b) del Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, acordó aprobar la política de protección de datos personales adjunta, que establece los principios, responsabilidades y pautas generales que deben regir el tratamiento de datos personales por Autoridad Portuaria de Gijón y tiene por objeto fijar un marco general para el tratamiento responsable, seguro y transparente de los datos personales y sentar las bases para garantizar que el tratamiento de datos personales realizado por la APG se lleva a cabo con respeto de los derechos de las personas, en particular de su privacidad, así como asegurar el cumplimiento de la normativa aplicable durante todo el ciclo de vida de los datos.

Lo que se hace público para general conocimiento.

Gijón, 17 de agosto de 2026.

LA PRESIDENTA

Firmado electrónicamente

Puerto de Gijón

Autoridad Portuaria de Gijón

Política de protección de datos personales de la Autoridad Portuaria de Gijón

Aprobada en la sesión de 14 de agosto de 2026

del Consejo de Administración

ÍNDICE

DISPOSICIONES GENERALES

1. Objeto y finalidad

La presente Política establece los principios, responsabilidades y pautas generales que deben regir el tratamiento de datos personales por Autoridad Portuaria de Gijón (en adelante APG). Tiene por objeto fijar un marco general para el tratamiento responsable, seguro y transparente de los datos personales.

Su finalidad es sentar las bases para garantizar que el tratamiento de datos personales realizado por la APG se lleva a cabo con respeto de los derechos de las personas, en particular de su privacidad, así como asegurar el cumplimiento de la normativa aplicable durante todo el ciclo de vida de los datos.

2. Ámbito de aplicación

Esta Política será aplicable a todos los órganos, áreas, unidades, sistemas, proyectos, servicios y personas que traten datos personales bajo la responsabilidad de la APG, cualquiera que sea el soporte utilizado.

También se aplicará, en lo que corresponda, a quienes actúen como encargados o subencargados del tratamiento, a entidades vinculadas y a terceros que accedan a datos personales tratados por la APG por razón de una relación administrativa o contractual o de cualquier tipo de colaboración.

Esta Política se tendrá en cuenta al adquirir o contratar aplicaciones, servicios, productos y encargados del tratamiento, seleccionando únicamente soluciones y proveedores que ofrezcan garantías suficientes.

3. Marco normativo

El tratamiento de datos personales en la APG se realizará de conformidad con el Reglamento (UE) 2016/679, General de Protección de Datos, (RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y las demás disposiciones europeas, estatales o sectoriales aplicables.

En especial, el tratamiento de datos personales llevado a cabo en la APG se acomodará a las recomendaciones, guías, informes, estándares o referencias aprobados o publicados por la Agencia Española de Protección de Datos y otras entidades o agencias reguladoras o consultivas en materia de seguridad de la información.

4. Definiciones

A efectos de la aplicación de esta Política, se aplicarán las definiciones establecidas en el RGPD. Así de forma resumida, se entenderá por **dato personal** toda información sobre una persona física identificada o identificable; por **tratamiento**, cualquier operación realizada sobre datos personales; por **responsable**, quien determine los fines y medios del tratamiento; por **encargado**, quien trate datos por cuenta del responsable; por **interesado**, la persona a la que se refieren los datos; por **violación de seguridad**, cualquier destrucción, pérdida, alteración, comunicación o acceso no autorizado; y por **evaluación de impacto**, el proceso destinado a identificar y mitigar los riesgos elevados para los derechos y libertades de las personas.

PRINCIPIOS BÁSICOS

Cualquier tratamiento de datos personales realizado por la APG deberá respetar, como mínimo, los siguientes principios.

5. Principios del tratamiento

a) **Licitud y lealtad:** el tratamiento de datos será legítimo, lícito y leal conforme a la normativa de aplicación. Los datos personales serán tratados conforme a una base jurídica válida y recogidos para uno o varios fines específicos, acordes a la normativa. Cuando resulte obligatorio, de acuerdo con la normativa, deberá obtenerse el consentimiento de los interesados antes de recabar sus datos personales.

b) **Legitimidad de la fuente:** no se obtendrán datos de fuentes ilícitas o carentes de garantías suficientes.

c) **Transparencia:** se facilitará a los interesados la información sobre el tratamiento de sus datos de forma comprensible y accesible, conforme a la normativa aplicable y se pondrán a disposición de los interesados mecanismos sencillos y específicos para ejercer sus derechos y presentar consultas o reclamaciones relacionadas con la protección de sus datos personales. La APG publicará información clara, accesible y comprensible sobre sus tratamientos, responsables y canales de contacto.

d) **Limitación de la finalidad:** se recogerán para fines determinados, explícitos y legítimos y no se utilizarán de manera incompatible.

e) **Minimización:** solo se tratarán los datos adecuados, pertinentes y estrictamente necesarios para la finalidad para la que se recojan o traten.

f) **Exactitud:** los datos se mantendrán correctos y actualizados, rectificándose o suprimiéndose cuando proceda.

g) **Limitación de la conservación:** los datos no se mantendrán más tiempo del necesario, salvo obligación legal o necesidad de atender responsabilidades.

h) **Integridad, confidencialidad y disponibilidad:** los datos se protegerán mediante medidas técnicas y organizativas proporcionales al riesgo.

i) **Responsabilidad proactiva:** la APG adoptará y documentará medidas que permitan demostrar el cumplimiento normativo y de esta Política en el tratamiento de datos personales.

j) **Privacidad desde el diseño y por defecto:** la protección de datos se integrará desde el inicio en los procesos gestionados por la APG, en los sistemas utilizados y en los servicios prestados, en el ejercicio de las competencias y funciones legalmente atribuidas al organismo.

6. Privacidad desde el diseño y por defecto

La APG integrará la privacidad desde la concepción de cualquier tratamiento y durante todo el ciclo de vida de los sistemas, servicios y procesos, desde su análisis, diseño y desarrollo hasta su gestión, operación, mantenimiento y retirada. Este enfoque se basará en la gestión del riesgo y la responsabilidad proactiva, de modo que la privacidad sea un requisito funcional y organizativo propio y no una medida añadida con posterioridad.

Se tendrán en cuenta los siguientes principios:

a) **Proactivo, no reactivo; preventivo, no correctivo.** Se anticiparán los riesgos para los derechos y libertades antes de que se materialicen, mediante análisis tempranos, responsabilidades claras, indicadores y medidas preventivas sujetas a mejora continua.

b) **Privacidad como configuración predeterminada.** Por defecto, solo se recogerán, utilizarán, conservarán y harán accesibles los datos estrictamente necesarios para cada finalidad. Los accesos se limitarán conforme al principio de necesidad de conocer, se establecerán plazos de conservación y se impedirán vinculaciones no autorizadas entre fuentes de datos.

c) **Privacidad incorporada en el diseño.** Los requisitos de privacidad se integrarán desde la concepción en los requisitos funcionales y no funcionales, la arquitectura, los procesos y las prácticas de gestión. Las nuevas iniciativas incluirán análisis de riesgos y, cuando corresponda, evaluaciones de impacto, dejando constancia de las decisiones adoptadas.

d) **Funcionalidad total: enfoque de beneficio conjunto.** Se buscarán soluciones que hagan compatibles la privacidad, la seguridad, la usabilidad, la eficacia y las finalidades legítimas. Cuando una alternativa comporte riesgos innecesarios, se explorarán opciones menos intrusivas.

e) **Protección durante todo el ciclo de vida.** Las garantías se mantendrán desde la recogida hasta la supresión o anonimización, incluyendo registro, clasificación, uso, consulta, comunicación, conservación y destrucción. Se valorarán, entre otras medidas, la seudonimización, la anonimización, el cifrado, la separación lógica o física, los perfiles de acceso y la destrucción segura.

f) **Enfoque centrado en la persona.** Los sistemas y procesos se diseñarán teniendo en cuenta las necesidades y expectativas razonables de las personas.

Para materializar estos principios se considerarán conjuntamente los objetivos de confidencialidad, integridad, disponibilidad y resiliencia.

Se seleccionarán y aplicarán las siguientes estrategias de diseño de la privacidad de acuerdo con el contexto y el riesgo y, siempre que sea posible, se combinarán para obtener una protección integral.

Estrategias orientadas a los datos	
Estrategia	**Descripción**
Minimizar	Limitar la recogida y el tratamiento al menor número posible de personas, atributos y operaciones. Implica seleccionar únicamente lo necesario, excluir información irrelevante, reducir progresivamente los datos y eliminarlos cuando dejen de ser necesarios.
Ocultar	Reducir la exposición y evitar que los datos sean conocidos por personas no autorizadas. Comprende restringir accesos, cifrar, disociar identificadores, seudonimizar.
Separar	Mantener independientes los conjuntos de datos y los contextos de tratamiento para dificultar correlaciones.
Abstraer	Utilizar el nivel mínimo de detalle compatible con la finalidad.

Estrategias orientadas a los procesos	
Estrategia	**Descripción**
Informar	Facilitar información completa, clara, accesible y contextual sobre qué datos se tratan, para qué, durante cuánto tiempo, con quién se comparten y qué derechos existen; asimismo, explicar cambios relevantes y notificar incidentes cuando proceda.
Controlar	Proporcionar a las personas mecanismos efectivos para consentir, elegir opciones, revisar y actualizar datos, modificar preferencias, retirar el consentimiento y solicitar la supresión o el ejercicio de otros derechos.
Cumplir	Establecer procedimientos, recursos, formación y controles que aseguren la conformidad legal y la eficacia continuada de las medidas de privacidad.
Demostrar	Conservar evidencias trazables del cumplimiento mediante registros de decisiones, análisis de riesgos, evaluaciones de impacto, pruebas, auditorías, documentación de incidentes e informes.

CONDICIONES BÁSICAS DEL TRATAMIENTO

7. Finalidades y bases jurídicas

Los datos personales podrán tratarse, entre otras, para las siguientes finalidades:

a) Ejercer las competencias y funciones legalmente atribuidas a la APG.

b) Gestionar relaciones administrativas, contractuales, laborales, profesionales y cualquier instrumento de colaboración o coordinación administrativa o público-privada.

c) Tramitar expedientes, solicitudes, consultas, reclamaciones, procesos de selección, pagos y comunicaciones relacionadas con los servicios prestados por la APG y el desarrollo de sus funciones legales.

d) Cumplir obligaciones legales, regulatorias, contables, fiscales, de transparencia, archivo, supervisión y de integridad.

e) Garantizar la seguridad de personas, instalaciones, redes, sistemas y operaciones.

f) Prevenir, detectar e investigar incidentes o incumplimientos.

g) Realizar análisis, estadísticas, mediciones de calidad y mejora de procesos, operaciones y servicios, utilizando anonimización o seudonimización siempre que sea posible.

h) Enviar comunicaciones informativas o comerciales cuando exista una base jurídica válida y se respeten las preferencias de las personas.

i) Adoptar decisiones automatizadas únicamente con las garantías establecidas en esta Política y en la normativa aplicable.

La base jurídica podrá ser el consentimiento, la ejecución de un contrato, el cumplimiento de una obligación legal, la protección de intereses vitales, el cumplimiento de una misión de interés público o el ejercicio de poderes públicos, y el interés legítimo debidamente ponderado.

Cuando el tratamiento se base en el consentimiento, este será libre, específico, informado e inequívoco, se conservará evidencia de su obtención y podrá retirarse en cualquier momento sin afectar a la licitud del tratamiento previo.

8. Derechos de las personas

Las personas interesadas podrán ejercer los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad y, cuando proceda, retirada del consentimiento y derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados.

La APG habilitará procedimientos sencillos, accesibles y gratuitos, verificará la identidad de quien solicite el derecho con criterios proporcionales y responderá dentro de los plazos legales. Si una solicitud no pudiera atenderse, explicará los motivos y las vías de reclamación. La persona interesada podrá dirigirse a la persona Delegada de Protección de Datos y presentar una reclamación ante la autoridad de control competente.

9. Categorías, procedencia y calidad de los datos

Podrán tratarse, según cada procedimiento, operación o actividad, entre otros, datos identificativos y de contacto, firma y autenticación, datos profesionales, económicos, contractuales o imágenes.

Los datos se obtendrán de la persona interesada o su representante, de relaciones contractuales, de sistemas y servicios utilizados, de administraciones u organismos públicos, de registros y fuentes accesibles legítimamente y de terceros autorizados. Se informará sobre su procedencia cuando la normativa lo exija.

Las categorías especiales de datos y los datos relativos a condenas o infracciones solo se tratarán cuando exista habilitación legal y se aplicarán garantías reforzadas. La APG adoptará medidas razonables para asegurar la exactitud, actualización y trazabilidad de los datos.

10. Registro, análisis de riesgos y evaluación de impacto

La APG mantendrá y publicará un Registro de Actividades de Tratamiento con la información exigida legalmente y lo revisará cuando se produzcan cambios relevantes.

Los tratamientos se someterán a análisis de riesgos periódicos. Cuando por su naturaleza, alcance, contexto, fines o uso de nuevas tecnologías puedan entrañar un alto riesgo, se realizará previamente una evaluación de impacto de conformidad con lo que exija la normativa aplicable. Si persistiera un riesgo elevado que no pudiera mitigarse, se efectuará la consulta previa a la autoridad de control cuando proceda.

11. Conservación, bloqueo y supresión

Los datos se conservarán mientras sean necesarios para la finalidad que justificó su recogida y durante los plazos establecidos por la normativa aplicable. Una vez finalizado el tratamiento, se bloquearán cuando corresponda y quedarán disponibles únicamente para jueces, tribunales, Ministerio Fiscal, administraciones o autoridades competentes durante los plazos de prescripción. Transcurridos estos, serán suprimidos o anonimizados de forma segura.

12. Destinatarios, encargados y comunicaciones

Los datos solo se comunicarán a terceros cuando exista una base jurídica válida, sea necesario para gestionar una relación o procedimiento, o lo exija una obligación legal. Podrán ser destinatarios, según el caso, administraciones públicas, autoridades de control y supervisión, órganos judiciales, entidades colaboradoras, proveedores y otras personas interesadas legitimadas.

Antes de contratar a un encargado del tratamiento se comprobarán sus garantías. La relación se formalizará por escrito, delimitando objeto, duración, naturaleza, finalidad, categorías de datos, medidas de seguridad, confidencialidad, subcontratación, asistencia en derechos e incidentes, auditoría y destino de los datos al finalizar el servicio.

13. Decisiones automatizadas e inteligencia artificial

Los tratamientos automatizados,y el uso de sistemas de inteligencia artificial se someterán a los principios de necesidad, proporcionalidad, transparencia, calidad, seguridad, explicabilidad y supervisión humana.

Antes de su implantación se evaluarán los riesgos, incluidos posibles errores, discriminaciones o sesgos, y se documentarán los datos utilizados, la lógica general, las medidas de mitigación, la supervisión y el ciclo de vida del sistema. Cuando una decisión produzca efectos jurídicos o afecte significativamente a una persona y se base únicamente en un tratamiento automatizado, se aplicarán las excepciones y garantías legales, incluido el derecho a obtener intervención humana, expresar el propio punto de vista e impugnar la decisión.

14. Transferencias internacionales

Con carácter general, no están previstas las transferencias internacionales de datos en los tratamientos de la APG.

En todo caso, las transferencias de datos a un tercer país solo se realizarán cuando exista una decisión de adecuación, garantías apropiadas —como cláusulas contractuales tipo u otros instrumentos reconocidos— o una excepción legal aplicable. Se evaluarán las circunstancias de la transferencia y se adoptarán medidas complementarias cuando sean necesarias.

SEGURIDAD DE LA INFORMACIÓN

La APG aplicará medidas técnicas y organizativas adecuadas al riesgo para garantizar la confidencialidad, integridad, disponibilidad, autenticidad, resiliencia y recuperación de los datos. Estas medidas incluirán, según corresponda, control de accesos, gestión de identidades y privilegios, cifrado o seudonimización, copias de seguridad, registro de actividad, protección de redes y dispositivos, gestión de vulnerabilidades, continuidad, destrucción segura y pruebas periódicas de eficacia.

Los accesos se limitarán a las personas autorizadas y a la información necesaria para sus funciones. Las medidas se revisarán ante cambios tecnológicos, organizativos, normativos o de riesgo.

Toda persona incluida en el ámbito de aplicación de esta Política que conozca una pérdida, acceso indebido, divulgación, alteración o destrucción de datos personales deberá comunicarla inmediatamente por los canales internos. La APG registrará el incidente, contendrá sus efectos, investigará las causas, evaluará el riesgo y adoptará medidas correctoras.

Cuando proceda, notificará la violación a la autoridad de control dentro del plazo legal y la comunicará a las personas afectadas conforme a lo previsto en la normativa si existe un alto

riesgo para sus derechos y libertades, exponiendo la naturaleza del incidente y las medidas adoptadas o recomendadas.

ROLES Y RESPONSABILIDADES DE GOBERNANZA

La APG designa una persona Delegada de Protección de datos que ejercerás las funciones y responsabilidades previstas en la normativa de aplicación. Sus datos de contacto y los canales para consultas o reclamaciones se harán públicos.

Al respecto de la estructura de gobernanza, esta política constituye una normativa específica integrada en el marco general de seguridad y cumplimiento de la APG y se encuentra alineada con los principios organizativos del Esquema Nacional de Seguridad desplegados en la Política de Seguridad de la Información y los roles y responsabilidades definidos en la misma. En consecuencia, los responsables designados en la Política de Seguridad de la Información desarrollarán en el ámbito de sus atribuciones las funciones derivadas de la implantación de esta Política.

De esta forma, corresponderá al Comité de Seguridad de la Información la responsabilidad de impulsar el marco de control interno aplicable, aprobando la normativa de desarrollo de esta política que sea necesaria, supervisar los riesgos relevantes y la eficacia de las medidas de control implantadas, así como con carácter general impulsar cualesquiera acciones tendentes a garantizar el cumplimiento de esta política, incluyendo la promoción de buenas prácticas y criterios homogéneos para el tratamiento de datos personales y el impulso de acciones de concienciación y formación en la materia.

Cada área o unidad organizativa será responsable de identificar sus tratamientos, aplicar las instrucciones internas, mantener la información actualizada y consultar previamente cualquier iniciativa que pueda implicar riesgos relevantes. El personal tratará únicamente los datos necesarios para sus funciones y estará sujeto al deber de confidencialidad.

FORMACIÓN, CONCIENCIACIÓN Y DEBER DE COLABORACIÓN

La APG impartirá formación periódica y adaptada a las funciones del personal, promoverá la concienciación sobre privacidad y seguridad y exigirá la aceptación de compromisos de confidencialidad.

Todas las personas sujetas a esta Política deberán colaborar con las áreas competentes, facilitar información veraz y comunicar riesgos, dudas o incumplimientos.

SUPERVISIÓN, AUDITORÍA Y MEJORA CONTINUA

El cumplimiento de esta Política se verificará mediante controles, indicadores, revisiones y auditorías internas o externas. Las deficiencias detectadas darán lugar a planes de acción con responsables y plazos definidos. La APG podrá requerir evidencias de cumplimiento a encargados y terceros, de acuerdo con los contratos y la normativa.

El Comité de Seguridad de la Información deberá analizar, proponer y supervisar las revisiones de la presente política para la mejora continua, teniendo en cuenta la evolución tecnológica, los cambios regulatorios, los nuevos riesgos detectados, los incidentes relevantes y los nuevos procesos corporativos.

Esta política será revisada al menos cada dos años, o en el momento que se produzcan cambios relevantes en el marco normativo y tecnológico o en la estrategia corporativa de la APG.

Las propuestas de modificación que procedan se elevarán al Consejo de Administración de la APG para su aprobación.

APROBACION Y ENTRADA EN VIGOR

Esta Política fue aprobada por el Consejo de Administración de la Autoridad Portuaria de Gijón en su sesión de **14 de agosto de 2026**. Será aplicable desde esa fecha y permanecerá vigente hasta su modificación o sustitución por una nueva versión.

La APG difundirá su contenido, facilitará los medios necesarios para su cumplimiento y verificará su aplicación efectiva. Todas las personas incluidas en su ámbito de aplicación deberán conocerla y asumir las responsabilidades que les correspondan.