Política de protección de datos personales en la empresa

VanKing Celkar Group Prosta Spółka Akcyjna

De conformidad con el artículo 24 del Reglamento 2016/679, a partir del 25 de mayo de 2018 se introduce la Política de protección de datos personales

Índice

1. Disposiciones generales

1. El presente documento, titulado «Política de protección de datos personales» (en lo sucesivo, «Política») tiene por objeto constituir un mapa de requisitos, normas y reglamentos de protección de datos personales en la Entidad.
2. La presente Política es una política de protección de datos personales en el sentido del RGPD , el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) DOUE L 2016.119.1.
3. La política, que establece las normas de tratamiento y protección de datos en la Entidad, incluye, en particular:

- una descripción de las normas de protección de datos en la Entidad,
- referencias a anexos con detalles (procedimientos o instrucciones modelo relativos a ámbitos específicos de la protección de datos que requieren una precisión en documentos separados).

2. Definiciones

Siempre que en la Política se haga referencia a:

1. el Responsable del Tratamiento de Datos Personales (RTPD)/Entidad, se entiende VanKing Celkar Group Prosta Spółka Akcyjna con sede en Niepołomice, ul. Podłęska 25, 32-005 Niepołomice, inscrita en el Registro Mercantil llevado por el Juzgado de Primera Instancia de Krakow-Śródmieście en Krakow, Sala XII de lo Mercantil, con el número KRS 0001045488, NIP 6792691789, REGON 356291869;
2. Instrucciones: se entiende por ello las instrucciones que determinan la forma de gestionar el sistema informático utilizado para el tratamiento de datos personales, que han sido aceptadas por el ADO como documento vinculante en la Entidad;
3. Reglamento (RGPD): se entiende por tal el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) DOUE L 2016.119.1 de 04.05.2016;
4. datos personales: cualquier información sobre una persona física identificada o identificable («el interesado»); se considera identificable una persona física que puede ser identificada, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos específicos que determinen la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona física;

5. datos de categorías especiales: se entiende por tales los datos personales mencionados en el artículo 9, apartado 1, del RGPD, es decir, los datos que revelan el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical y los datos genéticos, datos biométricos para identificar de manera inequívoca a una persona física o datos relativos a la salud, la sexualidad o la orientación sexual de dicha persona;
6. datos penales: los datos mencionados en el artículo 10, apartado 1, del RGPD, es decir, datos relativos a condenas e infracciones
7. contraseña: se entiende por contraseña una secuencia de caracteres alfabéticos, numéricos o de otro tipo, conocida únicamente por el usuario, que le permite acceder a los datos personales tratados en el sistema informático
8. identificador: se entiende por tal una secuencia de caracteres alfabéticos, numéricos o de otro tipo que identifica de forma inequívoca a la persona autorizada para tratar datos personales en el sistema informático;
9. integridad de los datos: propiedad que garantiza que los datos personales no han sido modificados o destruidos de forma no autorizada.
10. integridad del sistema: se entiende por ello la propiedad que garantiza la inviolabilidad del sistema, la imposibilidad de cualquier modificación no autorizada,
11. soporte de datos: se entiende por soporte el medio utilizado para grabar y almacenar información, por ejemplo, memorias USB, discos, discos duros,
12. persona: se entiende por persona el interesado, salvo que el contexto indique claramente lo contrario;
13. destinatario de los datos: se entiende por destinatario de los datos a la persona física o jurídica, autoridad pública, servicio u otro organismo a los que se revelen los datos personales, independientemente de que sean terceros. No obstante, los organismos públicos que puedan recibir datos personales en el marco de un procedimiento específico de conformidad con el Derecho de la Unión o el Derecho de los Estados miembros no se consideran destinatarios; el tratamiento de esos datos por parte de dichos organismos públicos debe ser conforme con las disposiciones en materia de protección de datos aplicables a los fines del tratamiento.
14. confidencialidad de los datos: se entiende por tal la propiedad que garantiza que los datos no se divulguen a entidades no autorizadas;
15. encargo del tratamiento de datos personales: se entiende por tal la realización de actividades de tratamiento de datos personales por parte de un encargado del tratamiento para cuenta del responsable del tratamiento, sobre la base de una cláusula contractual adecuada que garantice las condiciones de seguridad de los datos personales de conformidad con las disposiciones de la Ley y el Reglamento, o sobre la base de un contrato escrito independiente de encargo del tratamiento de datos personales celebrado de conformidad con el artículo 28 del RGPD;
16. entidad encargada del tratamiento: se entiende por tal la persona u organización a la que la Entidad ha encomendado el tratamiento de datos personales,
17. personal: se entiende por tal las personas que prestan servicios a ADO en virtud de una relación laboral, contratos civiles (por ejemplo, contratos por obra o por encargo), empresarios que ejercen su actividad de forma personal y individual, personas en prácticas, becarios, personas destinadas a trabajar en el marco de contratos con agencias de trabajo temporal que realizan trabajos relacionados con el tratamiento de datos personales en las estructuras de ADO;
18. RCPD o Registro: se entiende como el Registro de Actividades de Tratamiento de Datos.

19. persona autorizada para el tratamiento de datos personales: se entiende por ello un miembro del personal al que el ADO ha otorgado por escrito una autorización nominal para el tratamiento de datos en la Entidad,
20. usuario: se entiende por tal la persona autorizada a la que el ADO ha asignado un identificador y una contraseña,
21. tratamiento de datos: operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales de forma automatizada o no automatizada, tales como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación mediante transmisión, difusión o cualquier otra forma de puesta a disposición, alineación o combinación, restricción, supresión o destrucción;
22. responsabilidad: se entiende como la propiedad que garantiza que las acciones de un sujeto puedan atribuirse de manera inequívoca solo a ese sujeto,
23. sistema informático del administrador de datos personales: se entiende por ello el equipo informático, el software, los datos explotados en un conjunto de dispositivos, programas, normas de tratamiento de la información y herramientas de software que cooperan entre sí y que se utilizan para el tratamiento de datos,
24. Compartir datos personales: se entiende por ello la transferencia, divulgación y difusión de datos personales al destinatario de los datos.
25. eliminación de datos: se entiende por ello la destrucción de datos personales o su modificación de tal manera que no permita determinar la identidad de la persona a la que se refieren los datos,
26. seudonimización: el tratamiento de datos personales de tal manera que ya no puedan atribuirse a una persona física concreta sin utilizar información adicional, siempre que dicha información adicional se conserve por separado y esté sujeta a medidas técnicas y organizativas que impidan su atribución a una persona física identificada o identificable;
27. autenticación: se entiende como la acción destinada a verificar la identidad declarada de una persona física o jurídica;
28. protección del sistema informático: se entiende por tal la aplicación de medidas administrativas, técnicas y físicas adecuadas para proteger los recursos técnicos y proteger contra la modificación, destrucción, acceso no autorizado y divulgación u obtención de datos personales, así como su pérdida;
29. recopilación de datos personales: se entiende por ello la obtención de datos de la persona a la que se refieren o de otras fuentes,
30. conjunto de datos personales: se entiende por ello un conjunto ordenado de datos personales accesibles según criterios específicos, independientemente de que dicho conjunto esté centralizado, descentralizado o disperso funcional o geográficamente,
31. Consentimiento del interesado: se entiende como una manifestación voluntaria, específica, informada e inequívoca de la voluntad por la que el interesado, mediante una declaración o una acción afirmativa clara, da su consentimiento para el tratamiento de sus datos personales.

3. Objetivo de la introducción de la Política, ámbito de aplicación, modificaciones y actualizaciones

1. El responsable del tratamiento de datos personales, concediendo especial importancia a la protección de los datos personales tratados en las estructuras de la Entidad, se compromete a tomar todas las medidas necesarias para prevenir los riesgos para la seguridad de los datos derivados de acontecimientos tales como:
   a) violación de la seguridad de los datos mediante su tratamiento no autorizado,
   b) la divulgación a personas no autorizadas de las normas de protección de datos aplicadas por el ADO,
   c) la dispersión intencionada o accidental de datos en Internet eludiendo las medidas de seguridad del sistema o aprovechando errores del sistema informático del ADO,
   d) impacto imprevisto de factores externos en los recursos del sistema informático, como incendios, inundaciones, catástrofes constructivas, asaltos, robos, allanamientos, actos terroristas,
   e) parámetros ambientales inadecuados que perturben el funcionamiento de los equipos informáticos (humedad excesiva o temperatura muy alta, influencia de campos electromagnéticos y otros),
   f) fallos de hardware o software que indiquen claramente violaciones deliberadas de la protección de datos, funcionamiento inadecuado de los procedimientos de mantenimiento, incluida la autorización para reparar equipos que contengan datos personales fuera de la sede del ADO,
   g) ataques desde Internet,
   h) incumplimiento de las normas establecidas en la documentación sobre protección de datos personales por parte de personas autorizadas, relacionado con el incumplimiento por su parte de las normas de protección de datos, en particular:
   i) finalización del trabajo o abandono del puesto de trabajo de forma contraria a los procedimientos,
   j) divulgación a personas no autorizadas de las normas de protección de datos aplicadas en la ADO.
2. ADO elabora, aprueba y garantiza la aplicación de la Política como expresión de su voluntad de implementar las disposiciones legales relativas a la protección de datos personales y con el fin de garantizar la protección de los datos personales de los que es responsable frente a todo tipo de amenazas internas y externas, conscientes o inconscientes.
3. Independientemente de la Política, se ha elaborado y aplicado una Instrucción para la gestión del sistema informático utilizado para el tratamiento de datos personales.
4. La protección de los datos personales se lleva a cabo mediante: medidas de seguridad físicas, procedimientos organizativos, software del sistema, aplicaciones y el comportamiento de las personas autorizadas.
5. Las medidas de seguridad indicadas anteriormente tienen por objeto garantizar la confidencialidad, integridad y responsabilidad de los datos personales tratados por el ADO, así como la integridad del sistema informático utilizado para dicho tratamiento.
6. Si las disposiciones de cualquier ley prevén una protección de datos personales más amplia que la del Reglamento, se aplicarán las disposiciones de dichas leyes.
7. Las normas establecidas en la Política se aplican a todos:
   a) los datos personales tratados en la Entidad, tanto en el caso de que sea el responsable del tratamiento, como en el caso de que trate datos que le hayan sido confiados en virtud de contratos celebrados con arreglo al artículo 28 del Reglamento,

b) los soportes de información, por ejemplo, papel, magnéticos, ópticos, etc., en los que se encuentran o se encontrarán datos personales,
c) ubicaciones: edificios y locales a disposición de la Entidad en los que se tratan o se tratarán datos personales,
d) las personas que forman parte del personal y otras personas que tienen acceso a los datos personales.

4. Protección de datos personales en la Entidad: principios generales

1. Pilares de la protección de datos en la Entidad:
2. Legalidad: el administrador vela por la protección de la privacidad y trata los datos de conformidad con la ley.
3. Seguridad: el ADO garantiza un nivel adecuado de seguridad de los datos, tomando medidas constantes en este ámbito.
4. Derechos de las personas: el ADO permite a las personas ejercer sus derechos y los hace valer.
5. Responsabilidad: el ADO documenta cómo cumple con sus obligaciones para poder demostrar su conformidad en cualquier momento.
6. Principios de protección de datos:
7. Los datos personales son:
   a) tratados de manera lícita, leal y transparente para el interesado («licitud, lealtad y transparencia»);
   b) recogidos con fines determinados, explícitos y legítimos, y no tratados posteriormente de manera incompatible con dichos fines («limitación del fin»);
   c) ser adecuados, pertinentes y limitados a lo necesario para los fines para los que se traten («minimización de datos»);
   d) serán exactos y, cuando sea necesario, se actualizarán; se tomarán todas las medidas razonables para que los datos personales que sean inexactos en relación con los fines para los que se tratan se supriman o rectifiquen sin demora («exactitud»);
   e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que se tratan («limitación del almacenamiento»);
   f) ser tratados de manera que se garantice la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidentales, mediante medidas técnicas u organizativas adecuadas («integridad y confidencialidad»).

5. Sistema de protección de datos.

El sistema de protección de datos de la Entidad consta de los siguientes elementos:

1. Inventario de datos. El ADO identifica los recursos de datos personales en la Entidad, las clases de datos, las relaciones entre los recursos de datos, identifica los modos de utilización de los datos (inventario), incluyendo:
   a) casos de tratamiento de datos de categorías especiales y datos penales,
   b) casos de tratamiento de datos de personas que la ADO no identifica
   c) casos de tratamiento de datos,
   d) el perfilado,
   e) la coadministración de datos.
2. Registro. La ADO elabora, lleva y mantiene el Registro de Actividades de Tratamiento de Datos Personales en la Entidad (Registro). El Registro es una herramienta para evaluar el cumplimiento de la protección de datos en la Entidad.
3. Fundamentos jurídicos. La ADO garantiza, identifica y verifica los fundamentos jurídicos del tratamiento de datos y los registra en el Registro, incluyendo:
   a) mantiene un sistema de gestión de consentimientos para el tratamiento de datos,
   b) inventaría y detallaría la justificación de los casos en los que la ADO trata datos sobre la base del interés legítimo de la ADO.
4. Servicio de derechos de las personas. El ADO cumple con las obligaciones de información respecto a las personas cuyos datos procesa y garantiza el servicio de sus derechos, atendiendo las solicitudes recibidas en este sentido, incluyendo:
   a) obligaciones de información. El ADO transmite a las personas la información requerida por la ley al recopilar datos y en otras situaciones, y organiza y garantiza la documentación del cumplimiento de estas obligaciones;
   b) posibilidad de ejecutar las solicitudes. El ADO verifica y garantiza la posibilidad de ejecutar eficazmente cualquier tipo de solicitud por su parte y por parte de sus encargados del tratamiento.
   c) Tramitación de solicitudes. ADO garantiza los recursos y procedimientos adecuados para que las solicitudes de las personas se tramiten en los plazos y de la forma exigidos por el RGPD y se documenten.
   d) Notificación de infracciones. El ADO aplica procedimientos que permiten determinar la necesidad de notificar a las personas afectadas por una infracción de datos identificada.
5. Minimización. El ADO cuenta con normas y métodos de gestión de la minimización (privacidad por defecto), entre los que se incluyen:
   a) normas de gestión de la adecuación de los datos,
   b) normas de regulación y gestión del acceso a los datos,
   c) normas gestión del período de conservación de los datos y verificación de la
   6. Seguridad. El ADO garantiza un nivel adecuado de seguridad de los datos, lo que incluye:
   a) realiza análisis de riesgos para las actividades de tratamiento de datos o sus categorías,
   b) realiza evaluaciones de impacto en la protección de datos cuando el riesgo de vulneración de los derechos y libertades de las personas es elevado,
   c) adapta las medidas de protección de datos al riesgo determinado,
   d) cuenta con un sistema de gestión de la seguridad de la información,

e) aplica procedimientos que permiten identificar, evaluar y notificar las violaciones de datos identificadas a la Autoridad de Protección de Datos - gestiona los incidentes.

7. Encargado del tratamiento. El ADO cuenta con normas para la selección de los encargados del tratamiento de datos para el responsable del tratamiento, requisitos relativos a las condiciones de tratamiento (contratos de encargo) y normas de verificación del cumplimiento de los contratos de encargo.
8. Exportación de datos. El ADO cuenta con normas para verificar si la Entidad transfiere datos a terceros países (es decir, fuera de la UE, Noruega, Liechtenstein e Islandia) o a organizaciones internacionales, y para garantizar las condiciones legales de dicha transferencia, si se produce.
9. Privacidad desde el diseño. El ADO gestiona los cambios que afectan a la privacidad. Para ello, los procedimientos de puesta en marcha de nuevos proyectos e inversiones en la Entidad tienen en cuenta la necesidad de evaluar el impacto del cambio en la protección de datos, el análisis de riesgos y la garantía de la privacidad (incluida la compatibilidad de los fines del tratamiento, la seguridad de los datos y la minimización) ya en la fase de diseño del cambio, la inversión o al inicio de un nuevo proyecto.

6. Obligaciones del responsable del tratamiento de datos personales

1. El responsable del tratamiento de datos personales lleva a cabo tareas en el ámbito de la protección de datos personales con el fin de garantizar el cumplimiento de las disposiciones del Reglamento, en particular:
   a) Supervisa la elaboración y actualización de la documentación relativa a la protección de datos personales, incluidas la Política y las Instrucciones.
   b) Supervisa el cumplimiento de las normas establecidas en la documentación sobre protección de datos, incluida la Política y las Instrucciones.
   c) Garantiza medidas técnicas y organizativas adecuadas a los riesgos y a la categoría de los datos tratados que garanticen la protección de los datos personales en la Entidad.
   d) Garantiza que las personas a las que se les va a conceder la autorización para tratar datos conozcan las disposiciones sobre protección de datos y las normas de protección de datos adoptadas en la Entidad, organizando para ellas cursos de formación impartidos por una persona con los conocimientos y competencias adecuados. El ADO puede impartir los cursos de formación personalmente. La ficha de formación en materia de protección de datos personales constituye el anexo n.º 1 de la Política.
   e) Toma todas las medidas necesarias para garantizar la seguridad adecuada de los datos personales, en particular contra:
   a) el acceso de personas no autorizadas,
   b) su sustracción por parte de personas no autorizadas,
   c) cambio incontrolado, pérdida,
   d) daño o destrucción.
   f) Garantiza la legalidad del tratamiento de datos personales en la Entidad y, en particular, se asegura de que:
      - sobre la base de una de las condiciones de legalización mencionadas en los artículos 6 o 9 del Reglamento,
      - de conformidad con la legislación vigente y las buenas prácticas,
      - de conformidad con los principios de finalidad, veracidad, adecuación y limitación temporal.
   g) Autoriza el tratamiento de los datos personales de los miembros del personal de la Entidad en un ámbito determinado individualmente.
   h) Supervisa y vela por la transferencia legal de datos personales (puesta a disposición y cesión).
   i) Proporciona a los usuarios puestos de trabajo adecuados, incluido el equipo informático, que permitan el tratamiento seguro y legal de los datos personales.
   j) Toma las medidas adecuadas en caso de violación o sospecha de violación de las normas de tratamiento seguro de datos personales.
   k) Realiza periódicamente verificaciones internas del cumplimiento de la normativa sobre protección de datos personales, incluyendo comprobaciones.
   l) Garantiza el correcto funcionamiento del sistema informático, de acuerdo con los objetivos del tratamiento de datos personales.
   m) Asigna a cada usuario un identificador y una contraseña para el sistema informático, realiza las modificaciones necesarias en los permisos y elimina las cuentas de los usuarios de acuerdo con las normas establecidas en las Instrucciones.

n) Da de baja a los usuarios.
o) Gestiona el sistema informático en el que se tratan los datos personales, utilizando una contraseña de administrador para acceder a todas las estaciones de trabajo y servidores desde la posición de administrador.
p) Realiza y supervisa la reparación, el mantenimiento y la eliminación de los equipos informáticos en los que se tratan los datos personales.
q) Realiza y ejerce supervisa la realización de copias de seguridad, su almacenamiento y la comprobación periódica de su idoneidad para la recuperación de datos en caso de fallo del sistema informático.
r) Forma a los usuarios en materia de procedimientos e instrucciones que garantizan la protección de los datos personales y verifica la correcta aplicación de dichos procedimientos e instrucciones.
s) Aclara todas las irregularidades e incidentes notificados relacionados con el tratamiento de datos mediante medios informáticos.

2. El ADO garantiza el respeto de los derechos de los interesados, en particular el derecho a obtener información sobre:
   a) el responsable del tratamiento de los datos,
   b) la finalidad, el alcance, la forma y la base jurídica del tratamiento de datos,
   c) el plazo durante el cual se tratan los datos y qué datos se tratan,
   d) la fuente de la que proceden los datos,
   e) el modo de acceso a los datos y sus destinatarios.
   f) el período durante el cual se conservarán los datos personales y, cuando no sea posible, los criterios para determinar dicho período;
   g) el derecho a solicitar al responsable del tratamiento el acceso a los datos personales del interesado, su rectificación, supresión o limitación del tratamiento, o el derecho a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
   h) si el tratamiento se basa en el artículo 6, apartado 1, letra a), o en el artículo 9, apartado 2, letra a), del RGPD, información sobre el derecho a retirar el consentimiento en cualquier momento sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
   i) el derecho a presentar una reclamación ante una autoridad de control;
   j) si el suministro de datos personales es un requisito legal o contractual o una condición para celebrar un contrato, y si el interesado está obligado a suministrarlos y cuáles son las posibles consecuencias de no hacerlo;
   k) la toma de decisiones automatizada, incluida la elaboración de perfiles y, al menos en esos casos, información significativa sobre las reglas en que se basa la toma de decisiones, así como sobre la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
3. La ADO garantiza el respeto de los derechos de los interesados en lo que respecta a:
   a) solicitar la completitud, actualización, rectificación, supresión, transferencia de datos, limitación del tratamiento
   b) presentar una solicitud motivada para que se cese el tratamiento de los datos,
   c) retirar el consentimiento para el tratamiento de datos personales.

4. El ADO garantiza que se cumplirá con la obligación de informar al interesado a que se refiere el artículo 13 del Reglamento.

7. Normas para la concesión de autorizaciones para el tratamiento de datos

1. Solo podrán procesar datos en la Entidad aquellas personas que hayan recibido formación en materia de procesamiento y protección de datos de conformidad con la Política y las Instrucciones, y a las que el ADO haya otorgado una autorización por escrito para el procesamiento de datos personales, cuyo modelo figura en el Anexo n.º 2 de la Política.
2. Todo empleado de ADO autorizado para el tratamiento de datos personales, tras recibir la autorización para el tratamiento de datos personales y completar la formación, presentará una declaración de confidencialidad por escrito, cuyo contenido se determinará en función del ámbito de responsabilidades del empleado en cuestión y cuyo modelo figura en el Anexo 3a y el Anexo 3b de la Política.
3. En caso de que se autorice el tratamiento de datos personales a una persona empleada en la Entidad en virtud de formas de empleo de derecho civil, se celebrará un acuerdo de confidencialidad con dicha persona, tras haberle otorgado el ADO por escrito la autorización correspondiente para el tratamiento de datos personales.
4. La autorización a la que se refiere el punto 1 debe estar vigente. En caso de ausencia prolongada de la persona autorizada o de cese en el desempeño de parte o la totalidad de las funciones que justifican la necesidad de autorizarla para el tratamiento de datos personales, la autorización deberá ser anulada.
5. La pérdida de los derechos de tratamiento de datos personales derivados de la autorización para el tratamiento de datos personales puede producirse por:
6. la rescisión de la relación laboral u otra relación jurídica que vincule a la persona autorizada con el ADO,
7. cambio de puesto de trabajo en la ADO, en el que no sea necesario tener acceso a los ficheros de datos personales, y el nuevo ámbito de actividades no implique obligaciones profesionales relacionadas con el tratamiento de datos personales,
8. infracción deliberada de las normas de protección de datos personales establecidas en el Reglamento, la Política y las Instrucciones.
9. En caso de pérdida de los derechos para el tratamiento de datos personales, el ADO está obligado a cancelar inmediatamente la autorización para el tratamiento de datos personales y a realizar cambios en el registro de personas autorizadas para el tratamiento de datos en la base de datos correspondiente.
10. El registro de autorizaciones que lleva el ADO se encuentra en el Anexo n.º 4 de la Política.

8. Fundamentos del tratamiento

1. El tratamiento de datos personales comunes es posible si se cumple una de las condiciones establecidas en el artículo 6 del Reglamento, es decir, solo cuando:
    a) el interesado ha dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
    b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado;
    c) el tratamiento es necesario para el cumplimiento de una obligación legal impuesta al responsable del tratamiento;
    d) el tratamiento es necesario para la protección de los intereses vitales del interesado o de otra persona física;
    e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
    f) el tratamiento es necesario para los fines de los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, salvo que prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
2. El tratamiento de categorías especiales de datos es posible si se cumple una de las condiciones establecidas en el artículo 9 del Reglamento, es decir, solo cuando:
    a) el interesado ha dado su consentimiento explícito para el tratamiento de esos datos personales para uno o varios fines específicos;
    b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos por parte del responsable del tratamiento o del interesado en el ámbito del Derecho laboral, la seguridad social y la protección social;
    c) el tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física, y el interesado está física o jurídicamente incapacitado para dar su consentimiento;
    d) el tratamiento se realiza en el marco de una actividad legítima realizada con las garantías adecuadas por una fundación, una asociación u otra entidad sin ánimo de lucro con fines políticos, ideológicos, religiosos o sindicales, siempre que el tratamiento se refiera exclusivamente a los miembros o antiguos miembros de dicha entidad o a personas que mantengan contactos permanentes con ella en relación con sus fines, y que los datos personales no se divulguen fuera de dicha entidad sin el consentimiento de las personas afectadas;
    e) el tratamiento se refiere a datos personales que han sido evidentemente hechos públicos por el interesado;
    f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones, o en el marco de la administración de justicia por los tribunales;

g) el tratamiento es necesario por razones de interés público importante, en virtud del Derecho de la Unión o de un Estado miembro, que sean proporcionadas al objetivo perseguido, no vulneren la esencia del derecho a la protección de datos y prevean medidas adecuadas y específicas para proteger los derechos fundamentales y los intereses del interesado;

h) el tratamiento es necesario para fines de prevención de la salud o medicina del trabajo, para evaluar la capacidad de un empleado para trabajar, para realizar diagnósticos médicos, para prestar asistencia sanitaria o seguridad social, para tratar o gestionar sistemas y servicios de asistencia sanitaria o seguridad social en virtud del Derecho de la Unión o de un Estado miembro o en virtud de un contrato con un profesional sanitario;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección contra amenazas transfronterizas graves para la salud o la garantía de unos altos niveles de calidad y seguridad de la asistencia sanitaria y de los productos sanitarios o medicamentos, en virtud del Derecho de la Unión o del Derecho de los Estados miembros;

j) el tratamiento es necesario para fines de archivo en interés público, para fines de investigación científica o histórica o para fines estadísticos, en virtud del Derecho de la Unión o del Derecho de los Estados miembros.

3. La ADO documenta en el Registro los fundamentos jurídicos del tratamiento de datos para cada una de las operaciones de tratamiento.

4. El ADO implementa métodos de gestión de consentimientos que permiten registrar y verificar el consentimiento de la persona para el tratamiento de sus datos específicos con un fin concreto, el consentimiento para la comunicación a distancia y el registro de la denegación del consentimiento, la retirada del consentimiento y otras acciones similares.

9. Recopilación y tratamiento de datos personales

Obtención de datos personales

1. Los datos personales tratados en la Entidad se obtienen directamente de las personas a las que se refieren o de otras fuentes, dentro de los límites permitidos por la ley. Uso de datos personales

1. Los datos personales recopilados se utilizan exclusivamente para los fines para los que fueron, son o serán recopilados y tratados. El responsable del tratamiento conserva los datos personales en una forma que permite identificar al interesado únicamente durante el tiempo necesario para alcanzar el fin para el que se tratan, de conformidad con la legislación nacional.
2. En caso de que sea necesario facilitar documentos y datos que contengan datos personales que no estén directamente relacionados con la finalidad de la divulgación, se deberá proceder a la anonimización de dichos datos personales.

Modo de gestión de los derechos de las personas y las obligaciones de información

1. La ADO vela por la claridad y el estilo de la información transmitida y la comunicación con las personas cuyos datos trata.
2. El ADO facilita a las personas el ejercicio de sus derechos mediante diversas medidas, entre ellas: la publicación en el sitio web de información o enlaces a información sobre los derechos de las personas, la forma de ejercerlos en la Entidad, incluidos los requisitos de identificación, los métodos de contacto con el ADO a tal fin y la posible lista de precios de las solicitudes adicionales.
3. El ADO se encarga de cumplir los plazos legales para el cumplimiento de sus obligaciones hacia las personas.
4. El ADO introduce métodos adecuados de identificación y autenticación de las personas para el ejercicio de los derechos individuales y el cumplimiento de las obligaciones de información.
5. Con el fin de ejercer los derechos de las personas, el ADO garantiza procedimientos y mecanismos que permiten identificar los datos de personas concretas tratados por el ADO, integrar dichos datos, introducir cambios en ellos y eliminarlos de forma integrada.
6. El ADO documenta el cumplimiento de las obligaciones de información, las notificaciones y las solicitudes de las personas. Obligación de información

1. En cada caso en que se recopilen datos directamente del interesado, el responsable del tratamiento informará al interesado de conformidad con el anexo n.º 9 de la Política.
2. En cada caso en que se recopilen datos de fuentes distintas al interesado, el responsable del tratamiento informará al interesado sin demora, a más tardar en el primer contacto con el interesado, de conformidad con el anexo n.º 10 de la Política.
3. En todos los casos en que se obtenga el consentimiento del interesado, se utilizarán las cláusulas de consentimiento de conformidad con el Anexo n.º 11 de Política. ADO informa a la persona sobre el cambio previsto con el fin de procesar los datos. ADO informa a la persona antes de revocar la restricción del procesamiento. ADO informa a los destinatarios de los datos sobre la rectificación, supresión o restricción del procesamiento de los datos (a menos que ello requiera un esfuerzo desproporcionado o sea imposible).
4. ADO informa a la persona sobre su derecho a oponerse al tratamiento de datos, a más tardar en el primer contacto con dicha persona.

El responsable del tratamiento informará sin demora injustificada a la persona sobre la violación de datos personales si ello puede suponer un alto riesgo de violación de los derechos o libertades de dicha persona.

10. Solicitudes de las personas.

El registro de la ejecución de las solicitudes de la persona afectada constituye el Anexo n.º 19 de la Política.

1. Derecho de acceso a los datos

   A petición de la persona interesada en acceder a sus datos, el Responsable del tratamiento informará a la persona afectada de si está tratando sus datos y le comunicará los detalles del tratamiento, de conformidad con el artículo 15 del RGPD (el alcance corresponde a la obligación de informar en el momento de la recogida de datos), y le dará acceso a los datos que le conciernen. El acceso a los datos puede realizarse mediante la entrega de una copia de los mismos, con la salvedad de que la copia de los datos entregada en ejercicio del derecho de acceso a los datos no será considerada por el Entidad como la primera copia gratuita a efectos del cobro de tasas por copias de datos.

2. Copias de los datos

   A petición de la persona, la Entidad le facilitará una copia de los datos que le conciernen y anotará el hecho de haber facilitado la primera copia de los datos. La Entidad establece y mantiene una lista de precios de las copias de datos, según la cual cobra las tasas por las copias de datos sucesivas. El precio de la copia de los datos se calcula sobre la base del coste unitario estimado de la tramitación de la solicitud de copia de los datos.

3. Rectificación de datos

   La Entidad rectificará los datos incorrectos a petición de la persona. La Entidad tiene derecho a negarse a rectificar los datos, a menos que la persona demuestre de manera razonable la incorrección de los datos cuya rectificación solicita. En caso de rectificación de los datos, la Entidad informará a la persona sobre los destinatarios de los datos, a petición de esta.

4. Completar los datos

   La Entidad completará y actualizará los datos a petición de la persona. La Entidad tiene derecho a negarse a completar los datos si ello fuera incompatible con los fines del tratamiento de datos (por ejemplo, la Entidad no está obligada a tratar datos que le sean innecesarios). La entidad puede basarse en la declaración de la persona para completar los datos, a menos que sea insuficiente a la luz de los procedimientos adoptados por la entidad (por ejemplo, en lo que respecta a la obtención de dichos datos), la ley o existan motivos para considerar que la declaración no es fiable.

5. Eliminación de datos

   A petición de la persona, el Entidad eliminará los datos cuando:

   a) los datos personales ya no sean necesarios para los fines para los que fueron recogidos o tratados de otro modo;
   b) la persona haya retirado el consentimiento en el que se basa el tratamiento y no exista otra base jurídica para el tratamiento;
   c) la persona se ha opuesto eficazmente al tratamiento de dichos datos;
   d) los datos personales se hayan tratado de forma ilícita;
   e) los datos personales deben suprimirse para cumplir una obligación legal prevista en la ley;
   f) la solicitud se refiere a datos de un niño recopilados sobre la base del consentimiento para la prestación de servicios de la sociedad de la información ofrecidos directamente al niño. El responsable determina la forma de ejercer el derecho de supresión de datos de manera que se garantice el ejercicio efectivo de dicho derecho, respetando todas las normas de protección de datos, incluida la seguridad, y verificando que no se dan las excepciones contempladas en el artículo 17, apartado 3, del RGPD.

Si los datos que deben eliminarse han sido hechos públicos por la Entidad, esta tomará medidas razonables, incluidas medidas técnicas, para informar a otros responsables del tratamiento de dichos datos personales de la necesidad de eliminarlos y acceder a ellos. En caso de eliminación de los datos, la Entidad informará a la persona sobre los destinatarios de los datos, a petición de esta.

6. Limitación del tratamiento

   La Entidad limitará el tratamiento de los datos a petición de la persona cuando:

   a) la persona impugna la exactitud de los datos personales, durante un período que permita al responsable del tratamiento verificar la exactitud de dichos datos;
   b) el tratamiento es ilegal y la persona se opone a la supresión de los datos personales, solicitando en su lugar la limitación de su uso;
   c) el responsable ya no necesita los datos personales, pero son necesarios para que el interesado pueda formular, ejercer o defender sus derechos;
   d) la persona se ha opuesto al tratamiento por motivos relacionados con su situación particular, hasta que se determine si los motivos legítimos del Responsable prevalecen sobre los motivos de oposición de la persona afectada.

   Durante la limitación del tratamiento, el responsable del tratamiento conservará los datos, pero no los tratará (no los utilizará ni transmitirá) sin el consentimiento del interesado, salvo para la formulación, el ejercicio o la defensa de reclamaciones, o para la protección de los derechos de otra persona física o jurídica por motivos de interés público de importancia fundamental. El responsable del tratamiento informará a la persona antes de levantar la limitación del tratamiento. En caso de limitación del tratamiento de los datos, el responsable del tratamiento informará a la persona sobre los destinatarios de los datos, a petición de esta.

7. Transferencia de datos

   A petición de la persona, el Administrador emitirá, en un formato estructurado, de uso común y legible por máquina, o transmitirá a otra entidad, si es posible, los datos personales que le conciernen y que haya facilitado al ADO, tratados sobre la base del consentimiento de dicha persona o con el fin de celebrar o ejecutar un contrato celebrado con ella en los sistemas informáticos de la Entidad. La solicitud de transferencia de datos constituye el Anexo n.º 20 de la Política.

8. Oposición en una situación especial

   Si una persona presenta una oposición al tratamiento de sus datos motivada por su situación particular, y los datos son tratados por el Responsable del tratamiento sobre la base de un interés legítimo del Responsable del tratamiento o de una tarea encomendada al Responsable del tratamiento en interés público, el Responsable del tratamiento tendrá en cuenta la oposición, salvo que existan motivos legítimos imperiosos por parte del Responsable del tratamiento para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del solicitante de la oposición o motivos para la determinación, reclamación o defensa de derechos.

9. Oposición en investigaciones científicas, históricas o con fines estadísticos

   Si el Entidad realiza investigaciones científicas o históricas o trata datos con fines estadísticos, la persona puede presentar una oposición motivada por su situación particular a dicho tratamiento. El Administrador tendrá en cuenta dicha oposición, a menos que el tratamiento sea necesario para el cumplimiento de una tarea realizada en interés público.

10. Oposición al marketing directo

    Si la persona se opone al tratamiento de sus datos por parte del responsable del tratamiento con fines de marketing directo (incluido, en su caso, el perfilado), el responsable del tratamiento tendrá en cuenta la oposición y dejará de realizar dicho tratamiento.

11. Información y comunicación transparentes y modo de ejercicio de los derechos por parte del interesado

    El responsable del tratamiento tomará las medidas adecuadas para proporcionar al interesado, de forma concisa, transparente, inteligible y fácilmente accesible, en un lenguaje claro y sencillo, en particular cuando la información se dirija a un niño, toda la información a que se refieren los artículos 13 y 14 del RGPD, y mantendrá con él toda la comunicación relativa al tratamiento. La información se facilitará por escrito o por otros medios, incluidos, cuando proceda, los medios electrónicos. Si el interesado lo solicita, la información podrá facilitarse verbalmente, siempre que se confirme la identidad del interesado por otros medios.

    El responsable del tratamiento facilitará al interesado el ejercicio de los derechos que le asisten en virtud del RGPD.

    El administrador, sin demora injustificada y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud, informará al interesado de las medidas adoptadas en relación con la solicitud con arreglo a los puntos 1 a 11 anteriores. Si es necesario, este plazo podrá prorrogarse otros dos meses debido a la complejidad de la solicitud o al número de solicitudes. En el plazo de un mes a partir de la recepción de la solicitud, el responsable del tratamiento informará al interesado de dicha prórroga, indicando los motivos del retraso. Si el interesado ha presentado su solicitud por vía electrónica, la información se facilitará también por vía electrónica, siempre que sea posible, a menos que el interesado solicite otra forma.

    Si el Administrador no toma medidas en relación con la solicitud del interesado, informará inmediatamente, a más tardar en el plazo de un mes a partir de la recepción de la solicitud, al interesado de los motivos por los que no ha tomado medidas y de la posibilidad de presentar una reclamación ante la autoridad de control y de recurrir a las vías de recurso judiciales.

    La información facilitada a la persona cuyos datos se recogen y la comunicación y las medidas adoptadas en virtud de los puntos 1 a 11 anteriores serán gratuitas. Si las solicitudes de la persona afectada son manifiestamente infundadas o excesivas, en particular por su carácter repetitivo , el responsable podrá:

    a) cobrar una tasa razonable, teniendo en cuenta los costes administrativos de facilitar la información, mantener la comunicación o tomar las medidas solicitadas; o

    b) denegar de tomar las medidas en relación la la solicitud. La obligación de demostrar que la solicitud es manifiestamente infundada o excesiva recae en el responsable del tratamiento.

    Si el responsable del tratamiento tiene dudas fundadas sobre la identidad de la persona física que presenta la solicitud a que se refieren los artículos 15 a 21 del RGPD, podrá solicitar la información adicional necesaria para confirmar la identidad del interesado.

12. Consentimiento para el tratamiento de datos personales

    Los materiales relacionados con actividades del Entidad distintas de las establecidas por ley solo podrán enviarse a aquellas personas que hayan dado previamente su consentimiento por escrito para el tratamiento de sus datos personales

con este fin.
Los candidatos a un puesto de trabajo en la Entidad en el proceso de selección están obligados a firmar un consentimiento por escrito para el tratamiento de sus datos personales.
Los documentos presentados para la selección se conservan en la unidad organizativa que trata estos datos y se incorporan al expediente personal del empleado.

11. Registro de actividades de tratamiento de datos

1. El RCPD es una forma de documentar las actividades de tratamiento, actúa como mapa de tratamiento de datos y es uno de los elementos clave que permiten aplicar el principio fundamental en el que se basa todo el sistema de protección de datos personales, es decir, el principio de responsabilidad.
2. El ADO lleva un registro en el que inventaría y supervisa la forma en que utiliza los datos personales.
3. El registro es una de las herramientas básicas que permiten al responsable del tratamiento cumplir con la mayoría de sus obligaciones en materia de protección de datos.
4. En el Registro, para cada actividad de tratamiento de datos que el ADO haya considerado independiente a efectos del Registro, se consigna como mínimo: el nombre de la actividad, la finalidad del tratamiento, la descripción de la categoría de personas, la base jurídica del tratamiento, especificando la categoría de interés legítimo del Entidad, si es la base del tratamiento de datos, la forma de recogida de los datos, descripción de las categorías de destinatarios, información sobre la transferencia fuera de la UE/EEE, descripción general de las medidas técnicas y organizativas de protección de datos.
5. El registro de las actividades de tratamiento de datos personales forma parte de la documentación sobre protección de datos.
6. El registro constituye el Anexo n.º 12 de la Política.
7. El administrador designa a un delegado de protección de datos en los casos indicados en el artículo 37 del RGPD y, en caso de no haberlo designado, lo explica. La documentación pertinente se encuentra en el anexo n.º 13.

12. Minimización

1. La entidad se encarga de minimizar el tratamiento de datos en lo que respecta a:
    a) la adecuación de los datos a los fines (cantidad de datos y alcance del tratamiento)
    b) acceso a los datos,
    c) tiempo de conservación de los

    datos. Minimización del alcance
2. La entidad ha verificado el alcance de los datos obtenidos, el alcance de su tratamiento y la cantidad de datos tratados en términos de adecuación a los fines del tratamiento en el marco del RGPD.
3. La entidad revisa periódicamente la cantidad de datos tratados y el alcance de su tratamiento al menos una vez al año.
4. La entidad verifica los cambios en la cantidad y el alcance del tratamiento de datos en el marco de los procedimientos de gestión del cambio (privacidad desde el diseño).

    Minimización del acceso
5. La entidad aplica restricciones al acceso a los datos personales: legales (obligaciones de confidencialidad, ámbitos de autorización), físicas (zonas de acceso, cierre de locales) y lógicas (restricciones de los derechos de acceso a los sistemas que tratan datos personales y a los recursos de red en los que residen los datos personales).
6. La entidad aplica controles de acceso físico.
7. La entidad actualiza los derechos de acceso cuando se producen cambios en la composición del personal y en las funciones de las personas, así como cambios en las entidades encargadas del tratamiento.
8. La entidad revisa periódicamente los usuarios establecidos de los sistemas y los actualiza al menos una vez al año.

    Minimización del tiempo
9. La entidad implementa mecanismos de control del ciclo de vida de los datos personales en la entidad, incluida la verificación de la utilidad futura de los datos en relación con los plazos y puntos de control indicados en el registro.
10. Los datos cuya utilidad se ve limitada con el paso del tiempo se eliminan de los sistemas de la Entidad, así como de los archivos secundarios y principales. Estos datos pueden archivarse y conservarse en copias de seguridad de los sistemas y la información procesada por la Entidad. Los procedimientos de archivo y uso de los archivos, así como de creación y uso de copias de seguridad, tienen en cuenta los requisitos de control del ciclo de vida de los datos, incluidos los requisitos de eliminación de datos.

13. Divulgación de datos

1. El acceso a los datos personales solo es posible si se cumple una de las condiciones mencionadas anteriormente para el tratamiento de datos personales.
2. El acceso a los datos personales solo podrá tener lugar tras la presentación de una solicitud, cuyo modelo figura en el anexo 5 de la Política, para la transmisión o el acceso a la información.
3. El ADO lleva un registro de las divulgaciones de datos personales con el fin de garantizar el control del proceso de divulgación. El modelo del registro figura en el Anexo 6 de la Política.
4. La solicitud de acceso a los datos personales debe contener información que permita localizar los datos personales solicitados en el fichero e indicar su alcance y finalidad.
5. Al facilitar los datos personales, se debe indicar que solo pueden utilizarse para los fines para los que se han facilitado.
6. En caso de solicitud de información sobre los datos personales tratados, presentada por escrito por la persona a la que se refieren los datos, la respuesta a la solicitud se dará en un plazo de 30 días a partir de la fecha de su recepción.
7. Se denegará el acceso a los datos personales cuando ello suponga una violación grave de los derechos personales del interesado o de otras personas, y cuando los datos personales no guarden una relación significativa con los motivos de la solicitud del solicitante.

14. Encargo del tratamiento de datos personales

1. La ADO podrá encargar el tratamiento de datos personales a otra entidad externa mediante un contrato celebrado por escrito, incluso en forma electrónica, cuyo modelo figura en el anexo n.º 7 de la Política.
2. La lista detallada de los ficheros de datos personales y de las entidades a las que se confía el tratamiento de los datos personales figura en el Anexo 8 de la Política.
3. La transferencia de los conjuntos de datos a un tercero para su tratamiento no supone un cambio en el ADO competente.
4. Si el tratamiento se realiza en nombre del ADO, este solo utilizará los servicios de aquellos encargados del tratamiento que ofrezcan garantías suficientes de que aplicarán las medidas técnicas y organizativas adecuadas para que el tratamiento cumpla los requisitos del RGPD y proteja los derechos de los interesados.
5. El encargado del tratamiento no podrá recurrir a los servicios de otro encargado del tratamiento sin el consentimiento previo, específico o general, por escrito, del responsable del tratamiento. En caso de consentimiento general por escrito, el encargado del tratamiento informará al responsable del tratamiento de cualquier cambio previsto en relación con la incorporación o sustitución de otros encargados del tratamiento, dando así al responsable del tratamiento la oportunidad de oponerse a dichos cambios.
6. El tercero al que se le haya encomendado el tratamiento de datos personales estará obligado a utilizar los datos que se le hayan confiado únicamente para los fines y en la medida indicados en el contrato celebrado con él, así como a mantener la confidencialidad de los datos personales que se le hayan confiado para su tratamiento.
7. El tercero al que se le ha confiado el tratamiento de datos está obligado, entre otras cosas, a:
    a) aplicar medidas técnicas y organizativas que garanticen la protección del tratamiento de los datos personales adecuada a los riesgos y a la categoría de datos protegidos y, en particular, debe proteger los datos contra el acceso de personas no autorizadas, la sustracción por parte de personas no autorizadas, el tratamiento que infrinja la Ley y la modificación, pérdida, daño o destrucción,
    b) elaborar y aplicar la documentación relativa al tratamiento y la protección de datos personales,
    c) garantizar que solo las personas autorizadas por el ADO puedan acceder al tratamiento de datos,
    d) llevar un registro de las personas autorizadas para tratar datos,
    e) obligación de las personas autorizadas para el tratamiento de datos personales de mantener la confidencialidad de dichos datos y de los métodos y medidas de seguridad.
    f) garantizar el control sobre qué datos personales, cuándo y quién los ha introducido en la base de datos y a quién se transmiten,
    g) informar al ADO sobre la situación de subcontratación e indicar en el contrato el nombre de la entidad, junto con sus datos de contacto, a la que se subcontratarán los datos personales.

15. Seguridad

1. La entidad garantiza un nivel de seguridad adecuado al riesgo de violación de los derechos y libertades de las personas físicas como consecuencia del tratamiento de datos personales por parte de la entidad.

Análisis de riesgos y adecuación de las medidas de seguridad

2. La entidad lleva a cabo y documenta análisis de la adecuación de las medidas de seguridad de los datos personales. Para ello:
3. La entidad garantiza un nivel adecuado de conocimientos sobre seguridad de la información, ciberseguridad y continuidad del funcionamiento, ya sea internamente o con el apoyo de entidades especializadas.
4. La Entidad clasifica los datos y las actividades de tratamiento en función del riesgo que representan.
5. La entidad realiza análisis de riesgo de violación de los derechos o libertades de las personas físicas para las actividades de tratamiento de datos o sus categorías. La entidad analiza las posibles situaciones y escenarios de violación de la protección de datos personales, teniendo en cuenta la naturaleza, el alcance, el contexto y los objetivos del tratamiento, el riesgo de violación de los derechos o libertades de las personas físicas con diferente probabilidad de ocurrencia y gravedad de la amenaza.
6. La entidad determina las medidas de seguridad organizativas y técnicas que pueden aplicarse y evalúa el coste de su implementación. Para ello, la entidad determina la idoneidad y aplica medidas y enfoques tales como:
   a) seudonimización,
   b) cifrado de datos personales,
   c) otras medidas de ciberseguridad que constituyen la capacidad de garantizar de forma continua la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento,
   d) medidas para garantizar la continuidad del funcionamiento y prevenir los efectos de los desastres, es decir, la capacidad de restablecer rápidamente la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico.

Evaluaciones de impacto en la protección de datos

7. La entidad evalúa las repercusiones de las operaciones de tratamiento previstas en la protección de datos personales cuando, según el análisis de riesgos, el riesgo de vulneración de los derechos y libertades de las personas es elevado.
8. La entidad aplicará la metodología de evaluación de impacto adoptada en la entidad. Medidas de seguridad
9. La entidad aplicará las medidas de seguridad establecidas en el marco de los análisis de riesgos y la adecuación de las medidas de seguridad, así como de las evaluaciones de impacto en la protección de datos.
10. Las medidas de seguridad de los datos personales forman parte de las medidas de seguridad de la información y de la ciberseguridad de la Entidad y se describen con más detalle en los procedimientos adoptados por la Entidad para estos ámbitos.

Notificación de violaciones

11. La Entidad aplica procedimientos que permiten identificar, evaluar y notificar las violaciones de datos identificadas a la Autoridad de Protección de Datos en un plazo de 72 horas desde que se detecta la violación.

16. Medidas técnicas y organizativas necesarias para garantizar la confidencialidad, integridad y responsabilidad del tratamiento de los datos

1. Medidas de seguridad organizativas:
   a) se ha elaborado y aplicado una política de protección,
   b) Se ha elaborado e implementado un manual de gestión del sistema informático,
   c) solo se ha permitido el tratamiento de datos a personas autorizadas por el ADO,
   d) se lleva un registro de las personas autorizadas para procesar datos,
   e) los miembros del personal y otras personas que tratan datos personales han sido informados de las normas relativas a la protección de datos personales y a la seguridad del sistema informático,
   f) los miembros del personal y otras personas que tratan datos personales están obligados a mantener su confidencialidad,
   g) el tratamiento de datos personales se realiza en condiciones que protegen los datos contra el acceso de personas no autorizadas,
   h) la presencia de personas no autorizadas en las instalaciones donde se tratan datos personales solo se permite en presencia de una persona empleada en el tratamiento de datos personales y en condiciones que garanticen la seguridad de los datos,
   i) se aplica se aplica se aplican los contratos de encargo del tratamiento de datos para la colaboración con subcontratistas que tratan datos personales,
   j) se realizan revisiones periódicas de la Política y las Instrucciones,
   k) la transferencia de datos personales a terceros (compartir y encargar) se supervisa y se lleva a cabo de conformidad con la legislación vigente.
2. Las medidas de seguridad física para la protección de datos personales se describen en el Anexo 14 de la Política.
3. Las medidas de seguridad de los equipos informáticos y de telecomunicaciones se aplican a los elementos físicos del sistema, sus conexiones y los sistemas operativos. La descripción detallada de las medidas de seguridad figura en las Instrucciones.
4. Las medidas de seguridad de las herramientas de software y las bases de datos (técnicas y de software) se aplican a los procedimientos, aplicaciones, programas y otras herramientas de software que procesan datos personales. La descripción detallada de las medidas de seguridad figura en la Instrucción.

17. Procedimiento de análisis de riesgos y plan de gestión de riesgos

1. El administrador de datos realiza un análisis de riesgos para los recursos que participan en los procesos utilizando el anexo n.º 15 de la Política.
2. El análisis de riesgos se lleva a cabo al menos una vez al año y constituye la base para actualizar el procedimiento de gestión de riesgos.
3. Sobre la base de los resultados del análisis de riesgos realizado, el Administrador de datos implementa medidas de gestión de riesgos.
4. En cada caso, el administrador de datos elige el método de gestión de riesgos y determina qué riesgos se tratarán primero y en qué orden.

18. Exportación de datos

1. La entidad registra en el Registro los casos de exportación de datos, es decir, la transferencia de datos fuera del Espacio Económico Europeo (EEE en 2017 = Unión Europea, Islandia, Liechtenstein y Noruega).
2. Para evitar situaciones de exportación no autorizada de datos, en particular en relación con el uso de servicios en la nube de acceso público (shadow IT), la Entidad verifica periódicamente el comportamiento de los usuarios y, en la medida de lo posible, proporciona soluciones equivalentes que cumplan con la legislación en materia de protección de datos.

19. Diseño de la privacidad

1. La Entidad gestiona los cambios que afectan a la privacidad de manera que se garantice la seguridad adecuada de los datos personales y se minimice su tratamiento.
2. A tal fin, las normas de ejecución de proyectos e inversiones de la Entidad se basan en los principios de seguridad de los datos personales y minimización, exigiendo la evaluación del impacto en la privacidad y la protección de datos, la consideración y el diseño de la seguridad y la minimización del tratamiento de datos desde el inicio del proyecto o la inversión.

20. Procedimiento DPIA (Evaluación de impacto en la protección de datos)

1. La ADO evalúa el impacto de las operaciones de tratamiento previstas en la protección de datos cuando, según el análisis de riesgos, el riesgo de vulneración de los derechos y libertades es elevado.
2. La DPIA se lleva a cabo cada vez que se produce un cambio significativo en el proceso de tratamiento de datos personales, por ejemplo, un cambio de proveedor de servicios, un cambio en la forma de tratar los datos o una sustitución de los recursos que participan en el proceso.
3. La DPIA se lleva a cabo junto con el análisis de riesgos al menos una vez al año en relación con los procesos que, como resultado de una DPIA realizada anteriormente, han demostrado un alto riesgo para los derechos y libertades de los interesados.
   Medidas de seguridad
4. La ADO aplica las medidas de seguridad establecidas en el marco del análisis de riesgos y la adecuación de las medidas de seguridad, así como de la evaluación del impacto en la protección de datos.
5. Las medidas de seguridad de los datos forman parte de las medidas de seguridad de la información y de la ciberseguridad de la Entidad.

21. Procedimiento a seguir en caso de violación de la seguridad de los datos personales

1. Una violación de la protección de datos personales es una violación de la seguridad que da lugar a la destrucción, pérdida, modificación, divulgación no autorizada o acceso no autorizado accidental o ilícito a datos personales transmitidos, almacenados o tratados de otro modo, y en particular:
   a) acceso no autorizado a los datos,
   b) pérdida de soportes,
   c) modificaciones no autorizadas o destrucción de datos,
   d) divulgación de datos a entidades no autorizadas,
   e) divulgación ilegal de datos,
   f) obtención de datos de fuentes ilegales.
2. En caso de detectarse una violación de la seguridad del sistema informático o de producirse una situación que pueda indicar una violación de la seguridad de los datos personales, todos los miembros del personal están obligados a interrumpir el tratamiento de los datos personales y a notificarlo inmediatamente al ADO o a su superior inmediato, y a seguir las decisiones que estos tomen.
3. La notificación de la violación de la protección de datos personales debe incluir:
   a) una descripción de los síntomas de la violación de la protección de datos personales,
   b) la descripción de la situación y el momento en que se detectó la violación de la protección de datos personales,
   c) la especificación de cualquier información relevante que pueda indicar la causa de dicha violación,
   d) la descripción de las medidas de seguridad del sistema conocidas por la persona y de todas las medidas adoptadas tras la revelación del incidente.
4. Entre las amenazas típicas para la seguridad de los datos personales se encuentran:
   a) protección física inadecuada de las instalaciones, los equipos y los documentos,
   b) protección inadecuada del equipo informático o del software contra la fuga, el robo y la pérdida de datos personales,
   c) incumplimiento de las normas de protección de datos personales por parte del personal.
5. Entre los incidentes típicos de seguridad de los datos personales se incluyen:
   a) incidentes fortuitos externos (incendio del edificio/local, inundación, corte de suministro eléctrico, pérdida de comunicación),
   b) sucesos fortuitos internos (fallos del servidor, ordenadores, discos duros, software, errores de los informáticos, usuarios, pérdida/extravío de datos),
   c) incidentes intencionados (intrusión en el sistema informático o en las instalaciones, robo de datos/equipos, fuga de información, divulgación de datos a personas no autorizadas, destrucción deliberada de documentos/datos, acción de virus y otro software malicioso).
6. En caso de detectarse una amenaza o un incidente, el ADO lleva a cabo una investigación para determinar la causa de la amenaza o el incidente, indicar sus posibles consecuencias y las medidas que deben adoptarse para remediar la situación.
7. El ADO también determina las personas responsables de la infracción, recaba pruebas sobre el caso y documenta sus conclusiones.

8. El ADO también es responsable de analizar los incidentes de seguridad o las amenazas a la protección de datos personales con el fin de determinar si es necesario adoptar medidas correctivas o preventivas. Si el ADO determina que es necesario, identifica el origen del incidente o la amenaza, el alcance de las medidas correctivas o preventivas, el plazo de ejecución y la persona responsable.
9. El ADO es responsable de supervisar la corrección y la puntualidad de las medidas correctivas o preventivas aplicadas.
10. En caso de violación de la protección de datos personales, el ADO lo notificará sin demora injustificada a la autoridad de control, a ser posible en un plazo máximo de 72 horas tras la constatación de la violación, salvo que sea improbable que dicha violación dé lugar a un riesgo de vulneración de los derechos y libertades de las personas físicas. La notificación transmitida a la autoridad de control después de 72 horas irá acompañada de una explicación de los motivos del retraso.
11. La notificación a que se refiere el punto 10 deberá, como mínimo:
    a) describir la naturaleza de la violación de la protección de datos personales, indicando, en la medida de lo posible, las categorías y el número aproximado de personas afectadas, así como las categorías y el número aproximado de registros de datos personales afectados por la violación
    b) incluir el nombre y los datos de contacto del delegado de protección de datos o indicar otro punto de contacto al que se pueda acudir para obtener más información;
    c) describir las posibles consecuencias de la violación de la protección de datos personales;
    d) describir las medidas aplicadas o propuestas por el responsable del tratamiento para remediar la violación de la protección de datos personales, incluidas, en su caso, las medidas destinadas a minimizar sus posibles efectos negativos.
12. Si no es posible facilitar la información al mismo tiempo, se podrá facilitar de forma sucesiva y sin demora injustificada.
13. Todas las acciones anteriores son registradas por el ADO. Una vez controlada la situación de emergencia, el ADO elabora un informe final en el que expone las causas y los efectos del incidente, así como las conclusiones, incluidas las relativas al personal, que limitan la posibilidad de que se repita el incidente en el futuro; el modelo de informe final figura en el anexo n.º 16 de la Política.
14. El registro de infracciones figura en el anexo n.º 17 de la Política.
15. Si la violación de la protección de datos personales puede suponer un alto riesgo de violación de los derechos o libertades de las personas físicas, el Administrador notificará sin demora innecesaria a la persona afectada dicha violación.
16. La notificación a que se refiere el apartado 15 describirá, en un lenguaje claro y sencillo, la naturaleza de la violación de la protección de datos personales y contendrá, como mínimo, la información y las medidas a que se refiere el apartado 15.
17. La notificación a que se refiere el apartado 15 no será necesaria en los siguientes casos:
    a) el responsable del tratamiento ha aplicado medidas técnicas y organizativas adecuadas y dichas medidas se han aplicado a los datos personales afectados por la violación, en particular medidas como el cifrado, que impiden que personas no autorizadas puedan acceder a dichos datos personales;
    b) el responsable del tratamiento ha aplicado posteriormente medidas que eliminan la probabilidad de un alto riesgo de violación de los derechos o libertades del interesado a que se refiere la letra a);

c) requeriría un esfuerzo desproporcionado. En tal caso, se emitirá un comunicado público o se aplicará una medida similar mediante la cual se informará a los interesados de manera igualmente eficaz.

18. Si el Administrador aún no ha notificado a la persona afectada la violación de la protección de datos personales, la autoridad supervisora, teniendo en cuenta la probabilidad de que dicha violación de la protección de datos personales suponga un alto riesgo, podrá exigirle que lo haga o podrá determinar que se cumple una de las condiciones mencionadas en el apartado 17.
19. El procedimiento a seguir en caso de violación de la protección de datos personales se encuentra en el Anexo n.º 21 de la Política.
20. La lista de control sobre cómo actuar en caso de violación de la protección de datos se encuentra en el Anexo n.º 22 de la Política.

22. Revisiones de la Política y auditorías del sistema

1. La Política debe revisarse/verificarse al menos una vez al año para comprobar su actualidad y la conformidad de lo declarado en ella con la ley. En caso de cambios significativos en el tratamiento de datos personales, el ADO puede ordenar la revisión de la Política según sea necesario.
2. Las siguientes personas están autorizadas para controlar el estado de la protección de datos personales en la Entidad:
   a) el ADO,
   b) las personas designadas por el ADO.
3. El ADO analiza si la Política y el resto de la documentación relativa a la protección de datos personales es adecuada para:
   a) cambios en la estructura del sistema informático,
   b) cambios organizativos en ADO, incluidos los cambios en la condición de las personas autorizadas para tratar datos personales,
   c) cambios en la legislación vigente.
4. Una vez al año se someten a control todos los sistemas informáticos que tratan datos personales, así como las medidas de seguridad física y personal.
5. El ADO elabora un plan de control teniendo en cuenta el alcance y las necesidades físicas, temporales y de personal.
6. Se someten a control los equipos, el sistema informático, la aplicación de las medidas de seguridad y el cumplimiento de la Política.
7. El ADO puede, según sea necesario, realizar una auditoría interna de la conformidad del tratamiento de datos con la normativa sobre protección de datos personales.
8. El alcance, el desarrollo y los resultados de la auditoría se documentan por escrito en un informe.
9. El ADO puede encargar la realización de una auditoría externa a una entidad especializada. El modelo de informe figura en el anexo n.º 18 de la Política.

23. Disposiciones finales

1. La presente Política es un documento interno y no puede ser divulgado a personas no autorizadas en ninguna forma.
2. El usuario está obligado a presentar una declaración en la que certifique que ha tomado conocimiento de las disposiciones del Reglamento y de las instrucciones vigentes en ADO, así como de su compromiso de cumplirlas.
3. La declaración que confirma que el usuario conoce las disposiciones legales relativas a la protección de datos personales y las instrucciones vigentes en ADO, así como su compromiso de cumplirlas, se conserva en el expediente personal del empleado.
4. Todas las regulaciones relativas a los sistemas informáticos especificadas en la Política se aplican también al tratamiento de datos personales en bases de datos mantenidas en cualquier otra forma.
5. Todas las personas autorizadas están obligadas a aplicar las disposiciones contenidas en la presente Política al tratar datos personales.
6. Los casos de incumplimiento injustificado de las obligaciones derivadas del presente documento podrán dar lugar a la responsabilidad de la persona en cuestión, en función de la relación jurídica que la vincule con el ADO.
7. En los asuntos no regulados en la Instrucción, se aplicarán las disposiciones del Reglamento y otros actos, incluidos los ejecutivos.

Lista de anexos a la Política

1. Anexo n.º 1 a la Política: Ficha de formación en materia de protección de datos personales
2. Anexo n.º 2 a la Política: Autorización para el tratamiento de datos
3. Anexo n.º 3a a la Política: Declaración de confidencialidad: personal
4. Anexo n.º 3b a la Política: Declaración de confidencialidad: personal técnico y de limpieza
5. Anexo n.º 4 a la Política: Registro de autorizaciones
6. Anexo n.º 5 a la Política: solicitud de acceso a los datos
7. Anexo n.º 6 a la Política: Registro de accesos
8. Anexo n.º 7 a la Política: modelo de contrato de encargo del tratamiento de datos personales
9. Anexo n.º 8 a la Política: Registro de encargamientos
10. Anexo n.º 9 a la Política: modelo de cláusula informativa 1
11. Anexo n.º 10 a la Política: modelo de cláusula informativa 2
12. Anexo n.º 11 a la Política: modelo de cláusula de consentimiento para el tratamiento de datos
13. Anexo n.º 12 a la Política: Registro de actividades de tratamiento
14. Anexo n.º 13 a la Política: Lista de control: designación del delegado de protección de datos
15. Anexo n.º 14 a la Política: Normas de protección de las instalaciones
16. Anexo n.º 15 a la Política: Análisis de riesgos
17. Anexo n.º 16 a la Política: modelo de informe de violación de la protección de datos
18. Anexo n.º 17 a la Política: registro de violaciones de la protección de datos personales
19. Anexo n.º 18 a la Política: Informe sobre la verificación de la conformidad del tratamiento de datos personales con las disposiciones sobre su protección
20. Anexo n.º 19 a la Política: Registro de la ejecución de las solicitudes del interesado
21. Anexo n.º 20 a la Política: solicitud de transferencia de datos
22. Anexo n.º 21 a la Política: Esquema de actuación en caso de violación de la protección de datos personales
23. Anexo n.º 22 a la Política: Lista de control: cómo actuar en caso de violación de la protección de datos