WHITEHOLE INVESTMENT PARTNERS, SGIIC, S.A.

POLÍTICA DE PROTECCIÓN DE DATOS

POLÍTICA DE PROTECCIÓN DE DATOS

CONTENIDO

1. INTRODUCCIÓN

Whitehole Investment Partners SGIIC, S,A., (en adelante, "Whitehole") es consciente de la importancia de proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

En el apartado 1 del art. 24 del 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 (en adelante, "el Reglamento") se indica lo siguiente: "*Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el propio Reglamento*". Como continuación a lo anterior, en el apartado 2 del citado artículo, se indica que "*Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos*".

A tenor de lo anterior, Whitehole ha desarrollado esta Política que tiene como objetivo establecer los principios, criterios y responsabilidades necesarios para garantizar que se cumple con lo establecido en el Reglamento Europeo de Protección de Datos (en adelante RGPD) y en la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDyGDD) en cuanto al tratamiento de los datos de carácter personal.

2. ÁMBITO DE APLICACIÓN

2.1. Ámbito de aplicación subjetivo

La presente Política se aplicará a todos los empleados, agentes y colaboradores externos de Whitehole, incluidos los miembros del Consejo de Administración.

Además, esta política se hará extensiva a todas las sociedades que formen parte del grupo empresarial de Whitehole de acuerdo con el artículo 42 del Código de Comercio sometidas a la misma normativa o normativa análoga, en la medida en que no dispongan de una política específica propia.

2.2. Ámbito de aplicación objetivo

Esta política se aplicará al tratamiento de datos de carácter personal, tanto automatizados como no automatizados, en el territorio español, y a toda modalidad de uso posterior de estos datos por Whitehole y su posterior comunicación de datos.

3. MARCO LEGAL

- Reglamento (UE) 2016/679 del Parlamento y del Consejo Europeo 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 (en adelante "**RGPD**").
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, "**LOPDyGDD**").

4. DESCRIPCIÓN

4.1 Principios del Tratamiento de datos por Whitehole

4.1.1. Calidad de los datos

En el tratamiento de los datos de carácter personal se asegurará que los mismos:

- Sean tratados de forma lícita, legal y transparente.
- Solo se recojan los adecuados, pertinentes y limitados a la finalidad para la que son tratados.
- Se recojan para los fines determinados, explícitos y legítimos, acordados con anterioridad al inicio del tratamiento e informados al interesado.
- Sean exactos. Es necesario mantener los datos actualizados.

4.1.2. Transparencia e información a los interesados

Atendiendo a lo dispuesto en el considerando 39 del RGPD: *"Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro."*

Previo a la recogida de datos de carácter personal, Whitehole informará al afectado de las distintas finalidades del tratamiento de sus datos y de la base de licitud del tratamiento, del tiempo que se conservarán, de los posibles destinatarios de los datos y transferencias internacionales, de la manera de poder ejercitar sus derechos, de los datos de contacto del Delegado de Protección de Datos de Whitehole (en adelante, "DPO"), y de la autoridad de control competente en materia de protección de datos.

Cualquier obtención de datos de un particular a través de fuentes de información externas o de terceros, requerirá la obtención del consentimiento expreso, de acuerdo a la legislación vigente.

4.1.3. Licitud en el tratamiento de datos

Para que el tratamiento de datos de carácter personal sea lícito, es necesario que esté legitimado por una de las siguientes bases legales:

- El consentimiento previo del interesado para las finalidades informadas.
- La ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
- El cumplimiento de una obligación legal, aplicable al responsable del tratamiento.
- La protección de intereses vitales del interesado o de otra persona física.
- El cumplimiento de una misión realizada en interés público.
- El interés legítimo del responsable, o de un tercero, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.

4.1.4. Seguridad y secreto de los datos

Whitehole establecerá las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos de carácter personal.

Entre estas medidas podemos encontrar las siguientes:

- La seudonimización y el cifrado de datos personales.
- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- En caso de incidente físico o técnico, poder restaurar el acceso a los datos. Realizar un control periódico de las medidas técnicas y organizativas adoptadas para garantizar la seguridad del tratamiento.
- Realizar un control periódico de las medidas técnicas y organizativas adoptadas para garantizar la seguridad del tratamiento.

Existe una importante interrelación entre la seguridad en el tratamiento de los datos y el deber de secreto, ya que junto con las medidas de seguridad se tiene que garantizar el secreto y la confidencialidad de los datos personales que se tratan.

Quienes traten datos de carácter personal están obligados a cumplir con el deber secreto en relación con cualquier dato del interesado, incluso después de finalizar su relación con este.

Whitehole obtendrá de sus empleados el compromiso por escrito de las obligaciones de secreto y confidencialidad que le sean de aplicación respecto a los datos de carácter personal a los que puedan tener acceso en el ejercicio de sus funciones.

4.1.5. Conservación de los datos

Los datos personales recogidos serán almacenados únicamente durante el tiempo necesario para el cumplimiento de las finalidades de tratamiento que fueron informadas al interesado. Del mismo modo, Whitehole podrá conservar la información concluidas las finalidades de tratamiento principales, siempre y cuando mantenga la información debidamente bloqueada y accesible exclusivamente para la atención de requerimientos de Autoridades Públicas y Entidades Reguladoras.

Whitehole cuenta con procedimientos de destrucción segura de la información y, cuando sea necesario, se solicitará la emisión de los certificados a una compañía especializada.

4.1.6. Cesión de datos personales a un tercero

En la cesión de datos, el responsable del tratamiento (cedente) transmite los datos a un tercero (cesionario), previa notificación y consentimiento del interesado, con el objetivo de que el cesionario los use con una finalidad autónoma, trabajando por su cuenta y riesgo.

Para que se pueda dar la cesión de los datos será necesario que Whitehole informe a los interesados de la finalidad del tratamiento de sus datos, de la identidad del cesionario y haber recogido el consentimiento de los interesados. En cuanto al consentimiento, existen excepciones donde se pueden ceder datos a terceros sin el consentimiento de los interesados y serían los siguientes supuestos:

- En el caso de que la cesión esté autorizada por la Ley.
- Cuando la cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de datos, limitándose a la finalidad que la justifique.
- Cuando el cesionario sea el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas o las instituciones autonómicas con funciones análogas de las funciones que la ley les atribuye expresamente.
- Cuando la cesión se haga entre Administraciones públicas para el ejercicio de competencias similares y para los supuestos donde la finalidad del tratamiento sea con fines históricos, estadísticos o científicos.

- Cuando la cesión se haga respecto de datos de salud con la finalidad de proteger intereses vitales de los interesados necesarios para la prevención o el diagnóstico médico.
- Cuando los cesionarios sean las Fuerzas y Cuerpos de Seguridad del Estado, siempre que la cesión sea necesaria para prevenir un peligro real para la seguridad pública o para la represión de acciones penales.

Al margen de lo anterior, Whitehole siempre tendrá en cuenta el principio de minimización, de manera que solo se cederán los datos estrictamente necesarios, atendiendo a la finalidad y a la base legal que justifique la cesión de los datos.

4.1.7. Categorías Especiales de datos

Whitehole no tratará datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Como excepción a lo anterior, Whitehole podrá tratar los datos indicados anteriormente en los siguientes supuestos:

- Cuando el interesado haya dado su consentimiento para el tratamiento de esos datos, salvo que el Derecho de la Unión o de los Estamos miembros establezca que no se puede levantar la prohibición.
- Cuando el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, si así lo autoriza el Derecho de la Unión de los Estados miembros o un convenio colectivo.
- Cuando el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.
- Cuando el tratamiento sea efectuado por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.
- Cuando el tratamiento se refiera a datos personales que el interesado haya hecho manifiestamente públicos.
- Cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.
- Cuando el tratamiento sea necesario por razones de interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, debiendo ser proporcional al objetivo perseguido, respetando en lo esencial el derecho a la protección de datos y estableciendo medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.
- Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.
- Cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados

miembros, estableciendo medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

- Cuando el tratamiento sea necesario con fines de archivo en interés púbico, fines de investigación científica o histórica o fines estadísticos, respetando la protección de datos y estableciendo medidas para proteger los intereses y los derechos fundamentales del interesado.

4.2 Tratamiento de datos por parte de los empleados de Whitehole

El usuario que trate datos personales en sus funciones diarias tiene que conocer en detalle el correcto tratamiento y flujo de dichos datos, como pueden ser los canales de obtención, uso y almacenamiento, comunicación, acceso por parte de terceros prestadores de servicio, transferencias internacionales y destrucción de dichos datos personales.

Whitehole proporciona a todos los empleados (y eventualmente al personal externo) herramientas de trabajo que procesan datos de carácter personal, tales como cuentas de correo electrónico, dispositivos como ordenadores y teléfonos móviles, acceso a software y otras herramientas profesionales. Asimismo, la utilización de internet reviste de especial importancia por ser un canal de acceso de posibles amenazas como malware, virus y códigos maliciosos que pueden poner en peligro la integridad, disponibilidad y confidencialidad de los sistemas de Whitehole.

La correcta utilización de todos estos soportes y software es fundamental para garantizar la seguridad y el adecuado tratamiento de los datos personales y de la información confidencial.

En este sentido, Whitehole cuenta con medidas de seguridad técnicas adecuadas como antivirus, firewalls y registros de navegación de los usuarios, además de medidas de seguridad organizativas, reguladas en diferentes normas de obligado cumplimiento accesibles a todos los empleados a través de Sharepoint.

4.2.1 Bases de legitimación para el tratamiento de datos personales

- **Consentimiento**

En el RGPD se define el consentimiento del interesado como *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen."*

Cuando el tratamiento de los datos personales se base en el consentimiento que dio el interesado, Whitehole deberá poder acreditar la existencia del mismo, que fue libremente prestado, esto es, que el no otorgarlo no acarrearía consecuencias negativas para el interesado y que fue prestado para cada una de las finalidades, teniendo la opción de poder revocarlo en cualquier momento, sin que la revocación pueda afectar a la licitud del tratamiento basada en el consentimiento previo a su retirada.

Si el consentimiento fuera revocado, Whitehole dejará de tratar los datos respecto de la finalidad o tratamiento respecto de cual el consentimiento haya sido revocado.

Para la obtención del consentimiento será necesario que Whitehole facilite, al menos, la información indicada en el art. 13 del RGPD (ver punto 4.2.2), así como cualquier información necesaria que permita al interesado consentir de manera informada y libre el tratamiento de sus datos para las finalidades previstas mediante una clara acción afirmativa.

Cuando el tratamiento tenga varias finalidades, deberá darse el consentimiento para cada uno de ellos.

- **Ejecución de un contrato**

Cuando Whitehole pueda basar el tratamiento de los datos de los interesados en la ejecución de un contrato en el que el interesado sea parte o para la aplicación a petición de estos de medidas precontractuales, los datos tratados serán los imprescindibles para la ejecución, desarrollo y mantenimiento del contrato.

En el supuesto en el que se recaben consentimientos durante la formalización de un contrato para finalidades que no tengan que ver con el mismo, Whitehole establecerá mecanismos para que el interesado pueda manifestar su negativa a dar el consentimiento.

Si los datos personales han sido facilitados por el interesado para la aplicación de medidas precontractuales y luego el contrato no se formaliza, Whitehole no podrá tratar esos datos, salvo que el interesado haya consentido su posterior conservación y tratamiento o exista una obligación legal que lo permita.

- **Cumplimiento de una obligación legal**

Cuando Whitehole pueda basar el tratamiento de los datos personales de los interesados en el cumplimiento de una obligación legal, proporcionará información actualizada sobre las novedades legislativas, tanto comunitarias como nacionales, que le sean de aplicación y que suponga el tratamiento de datos personales para dar cumplimiento a una obligación legal.

- **Interés legítimo**

El interés legítimo es una de las bases de legitimación del tratamiento que permitirá tratar los datos personales a Whitehole cuando sea *"necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales".*

Para que Whitehole pueda basar el tratamiento de datos personales en su interés legítimo o en el de un tercero, deberá realizar, con anterioridad al tratamiento, un análisis de ponderación del riesgo entre el interés legítimo de quien va a tratar los datos personales y los intereses y derechos fundamentales del interesado. Ponderar todas estas circunstancias en conjunto hará posible establecer si el interesado está habilitado para ejecutar ciertas actividades de tratamiento sobre los datos personales de un tercero, sin que este haya dado su consentimiento.

Existe interés legítimo cuando el tratamiento se realiza en el marco de la relación con un cliente, cuando trata los datos personales para fines de mercadotecnia directa, para prevenir el fraude o para garantizar la seguridad de la red y la información de sus sistemas informáticos.

4.2.2 Información a los interesados sobre el tratamiento de sus datos personales

En el art. 13 y 14 del GDPR se recoge la información que se debe proporcionar al interesado, en función de si los datos personales se obtienen del interesado o no.

Se informará al interesado de las circunstancias y condiciones del tratamiento que se va a realizar de sus datos y de los derechos que le asisten atendiendo a lo dispuesto en el RGPD y LOPDyGDD.

Al interesado se le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el interés legítimo, se informará los intereses legítimos del responsable o del tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) la intención del responsable de transferir datos personales a un tercer país u organización internacional;

g) el plazo durante el cual se conservarán los datos;

h) los derechos que puede ejercitar el interesado (acceso, rectificación, supresión, limitación y oposición);

i) el derecho a presentar una reclamación ante una autoridad de control;

j) consecuencias de no facilitar los datos personales si la comunicación de datos personales es un requisito legal o contractual.

En el caso de que los datos personales no se hayan obtenido del interesado, se deberá informar en los mismos términos señalados anteriormente, en el plazo de un mes desde la obtención de los datos y además habrá que informar sobre la fuente de la que proceden los datos personales y si se trata de fuentes públicas.

4.2.3 Ejercicio de derechos en protección de datos

Whitehole como Responsable del Tratamiento tiene la obligación de establecer fórmulas para facilitar a los interesados el ejercicio de sus derechos reconocidos en el RGPD y en la LOPDyGDD, y que permitan al interesado defender su privacidad y controlar por sí mismo el uso que se hace de sus datos personales. En este sentido, cualquier interesado tiene el derecho y la capacidad de conocer, modificar, limitar y/o suprimir los datos de carácter personal, así como a exigir su limitación durante ciertos períodos de tiempo.

Los derechos que podrán ejercitar los interesados son los siguientes:

- **Acceso**: el interesado tendrá derecho a obtener de Whitehole cuando sea responsable del tratamiento, confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales.
- **Rectificación**: el interesado tendrá derecho a obtener de And Whitehole bank la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta las finalidades del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, incluso mediante una declaración adicional.
- **Supresión**: el interesado tendrá derecho a obtener sin dilación indebida de Whitehole la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir los datos cuando concurra alguna de las circunstancias siguientes:
    - los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo:
    - el interesado retire el consentimiento en que se basa el tratamiento, y este no se base en otro fundamento jurídico;
    - el interesado se oponga al tratamiento cuando la base legitimadora del mismo sea el interés público o el interés legítimo, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento cuando el tratamiento tenga por objeto la mercadotecnia directa;
    - los datos personales hayan sido tratados ilícitamente:
    - los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
    - los datos personales se hayan obtenido en relación con la oferta directa a niños de servicios de la sociedad de la información (art. 8.1 RGPD).

  Si se han hecho públicos los datos personales y procede la supresión de los mismos, Whitehole adoptará las medidas razonables, para informar a quienes estén tratando dichos datos de la solicitud de supresión del interesado.

  Al margen de lo anterior, el art. 17 del RGPD establece excepciones al ejercicio del derecho de supresión y no se podrá realizar la supresión cuando el tratamiento sea necesario:

  - para ejercer el derecho a la libertad de expresión e información;
  - para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento,

o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

- por razones de interés público en el ámbito de la salud pública;
- con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho de supresión pudiera hacer imposible obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
- para la formalización, el ejercicio o la defensa de reclamaciones.

Whitehole no podrá, en la mayoría de los casos, dar curso al ejercicio de supresión porque los tratamientos efectuados son necesarios para el cumplimiento de obligaciones legales y para la defensa de reclamaciones.

- **Limitación del tratamiento:** el interesado tendrá derecho a obtener de Whitehole la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:
    - el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
    - el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
    - el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamación;
    - el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

  Una vez atendido el derecho de limitación, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

- **Oposición**: el interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en el interés legítimo o en el interés público, incluida la elaboración de perfiles sobre la base de dichas disposiciones. Whitehole dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

  Whitehole cuando reciba la solicitud del ejercicio del derecho de oposición, comprobará que existe legitimación para el ejercicio, esto es, si el derecho de oposición se refiere a los tratamientos basado en el artículo 6.1e) (interés público) y 6.1f) (interés legítimo) del RGPD, incluido el tratamiento con fines basados en la mercadotecnia directa.

  El ejercicio del derecho de oposición no procederá por ej. cuando los datos se traten para finalidades como puedan ser la de evitar la corrupción, prevenir el blanqueo de capitales, controlar y prevenir el fraude.

  Una vez atendido el derecho de oposición, Whitehole deberá dejar constancia en sus sistemas, de manera que se impida el tratamiento de los datos personales.

- **Portabilidad de los datos**: el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

- el tratamiento esté basado en el consentimiento o sea necesario para la ejecución de en un contrato, y
- el tratamiento se efectúe por medios automatizados

Al ejercer su derecho a la portabilidad, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable, cuando sea técnicamente posible.

Los datos que se pueden portar son los aportados por el interesado cuya base legitimadora sea el consentimiento o la ejecución de un contrato. Es criterio de la Agencia Española de Protección de Datos que *"no son objeto del derecho de portabilidad aquellos datos que puedan ser considerados "inferidos" y "derivados", entendidos como los que resulten de la aplicación a la información generada en el desarrollo del servicio de conocimiento o técnicas propias del responsable; es decir, procedentes de la aplicación sobre los datos relacionados con el producto o servicio de técnicas que forman parte del know how del responsable (como pueden ser entre otros, técnicas matemáticas o resultantes de la aplicación de algoritmos)."*

En cuanto a la rectificación o supresión hay que tener en cuenta que el artículo 32 de la LOPDyGDD establece la obligación de bloquear los datos cuando se solicite su rectificación o supresión. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de la Agencia Española de Protección de Datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el párrafo anterior. Transcurrido el plazo establecido para el bloqueo, deberá procederse a la destrucción de los datos.

Whitehole cuenta con un Registro para documentar la debida atención de todas las solicitudes de ejercicio de derechos de protección de datos, cuya cumplimentación está supervisada por el Delegado de Protección de Datos.

La atención de los derechos de los interesados requiere la participación de todos los empleados de Whitehole, por lo que éstos deben conocer cómo actuar al recibir una solicitud de ejercicio de derechos.

4.2.4 Relación con terceros (encargados del tratamiento)

En ocasiones Whitehole puede apoyarse en servicios de terceras compañías que pueden llegar a acceder a datos personales de Whitehole.

No obstante, lo anterior, puede haber proveedores con los que pueda contar Whitehole que aun accediendo a información confidencial pueden no acceder a datos personales.

En cualquier caso, cuando un tercero deba acceder a los datos de carácter personal como consecuencia de la ejecución de un contrato, dicho acceso deberá regularse adecuadamente en el contrato que rija la prestación del servicio. El contrato deberá recoger, entre otras, las siguientes cuestiones: (i) objeto del contrato; (ii) duración; (iii) naturaleza; (iv) finalidad del tratamiento; (v) tipo de datos personales que se van a tratar; (vi) categorías de interesados; (vii) obligaciones y derechos del responsable.

Asimismo, en el contrato deberán constar las medidas de seguridad que deberá adoptar el encargado del tratamiento para garantizar el adecuado tratamiento y custodia de los datos. Por último, el proveedor, según se acuerde en el contrato, deberá destruir o devolver los datos una vez prestado el servicio.

La subcontratación de los servicios que suponga el acceso a datos personales por parte del encargado del tratamiento deberá ser autorizada por Whitehole y el subcontratista (subencargado del tratamiento) deberá tener las mismas obligaciones en materia de protección de datos que el encargado del tratamiento.

4.2.5 Medidas técnicas y organizativas

El RGPD indica que se debe establecer la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por el mismo o por su cuenta y debe aplicar las medidas oportunas, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo.

Dentro de las medidas que Whitehole adopta para garantizar el cumplimiento del RGPD se encuentran las siguientes:

- **Registro de actividades de tratamiento (RAT).** Whitehole lleva un registro de las actividades de tratamiento que realiza. El registro contiene la siguiente información:
    - Nombre y datos de contacto del responsable y, en su caso, del corresponsable, del representante, y del delegado de protección de datos.
    - Finalidades del tratamiento.
    - Categorías de destinatarios a quien se comunicaron o comunicarán los datos personales, incluidos los destinatarios de terceros países u organizaciones internacionales.
    - Transferencias internacionales de datos personales a un tercer país o a una organización internacional.
    - Cuando es posible, los plazos previstos para la supresión de las diferentes categorías de datos.
    - Cuando es posible, una descripción general de las medidas técnicas y organizativas de seguridad.

  El registro se actualiza y está a disposición de la autoridad de control que lo solicite.
- **Análisis de riesgo.** Cuando Whitehole actúe como responsable del tratamiento realizará un análisis de los riesgos que pueden entrañar las actividades que trata. La Agencia Española de Protección de Datos (en adelante, la "AEPD") indica que *"El análisis de riesgo supone un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles consecuencias que una actividad puede tener sobre un conjunto de bienes o elementos que han de ser protegidos."* Este análisis va a llevar a tomar decisiones que, en algunos casos, supongan desarrollar controles que minimicen el riesgo.
- **Protección de datos desde el diseño y por defecto.**
    - **Protección de datos desde el diseño.** El RGPD establece que *"…el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento y proteger los derechos de los interesados."*

      El principio de la protección de datos desde el diseño apuesta por tener en cuenta la privacidad a lo largo de todo el ciclo vital de un producto o servicio, desde su creación a su comercialización. Este nuevo enfoque proactivo nos permite prever y protegernos frente a los efectos negativos e invasivos de los nuevos productos y tecnologías desde el principio, partiendo de la minimización de los datos, tanto en lo que se refiere a la cantidad que se maneja como al tratamiento, el plazo de conservación y la accesibilidad.

      La aplicación del principio de la protección de datos desde el diseño, exigirá la evaluación de varios aspectos y objetivos concretos. A la hora de tomar decisiones sobre el diseño de un sistema de tratamiento, su adquisición y su funcionamiento, deberán respetarse los aspectos generales y los objetivos siguientes: (i) Minimización de los datos (tratar únicamente los datos

que sean precisos para cada uno de los fines específicos); (ii) Capacidad de control (tener un sistema de tecnología de la información que dote a los interesados de medios de control eficaces relativos a sus datos personales); (iii) Transparencia (los interesados deben estar suficientemente informados acerca de los medios de los sistemas); (iv) Facilidad de uso de los sistemas (las funciones y los mecanismos relativos a la privacidad deben ser fáciles de utilizar y deben proporcionar la ayuda suficiente a aquellos usuarios de menor experiencia; (v) Confidencialidad de los datos (se debe garantizar el secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito); (vi) Calidad de los datos (se da cuando los datos se ajustan al propósito para el que fueron destinados); (vii) Limitación del uso (los sistemas de tecnología de la información que puedan utilizarse con distintos fines o que se manejen en un entorno multiusuario deberán garantizar que los datos y los procesos que sirvan para distintas tareas o fines puedan separarse entre si de forma segura).

    - **Protección de datos por defecto.** Whitehole garantizará que solo serán objeto de tratamiento los datos personales que sean estrictamente necesarios para cada una de las finalidades establecidas.

- **Medidas de seguridad.** El art. 32 del RGPD establece que se deben adoptar las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

  Estas medidas deben incluir, entre otros:

    - la seudonimización y el cifrado de datos personales;
    - la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
    - la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
    - un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

  Whitehole, como responsable del tratamiento, debe establecer las medidas técnicas y organizativas adecuadas que debe implementar el encargado del tratamiento para cada tratamiento de datos personales establecido por Whitehole.

  El art. 30 del RGPD establece que dentro del Registro de actividades de tratamiento habrá que incluir, cuando se pueda, una descripción general de las medidas técnicas y organizativas de seguridad.

  El art. 42 del RGP establece la posibilidad de crear mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD.

- **Violaciones de seguridad de los datos.** El RGPD lo define como *"toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."*

  La no adopción de medidas técnicas y organizativas adecuadas puede dar lugar a violaciones de seguridad que produzcan *"daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobres sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto*

profesional, o cualquier toro perjuicio económico o social significativo para la persona física en cuestión."

Whitehole debe comunicar una violación de seguridad a la autoridad de control en cuanto tenga conocimiento de la misma y, en todo caso, en un plazo que no sea superior a 72 horas desde que haya tenido conocimiento de la misma, a menos que se pueda demostrar que la violación de la seguridad de los datos personales no va a suponer un riesgo para los derechos y libertades de las personas físicas.

La violación de seguridad se comunicará también al interesado cuando la misma suponga un riesgo alto para los derechos y libertades de las personas físicas. En este supuesto, el RGPD establece unas excepciones, donde no será necesario comunicar la violación de seguridad al interesado si se cumple alguna de las condiciones siguientes:

- que el responsable del tratamiento haya adoptado medidas técnicas y organizativas apropiadas y estas medidas se hayan aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
- que el responsable del tratamiento haya tomado las medidas ulteriores que garanticen que ya no existe la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado;
- que suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

La detección y gestión de violaciones de seguridad requiere la participación de todos los empleados de Whitehole, por lo que éstos deben conocer cómo actuar en caso de que Whitehole sufra una violación de seguridad.

- **Evaluación de impacto.** El art. 35 del RGPD establece que si es probable que un tratamiento de datos personales puede entrañar un alto riesgo para los derechos y libertades de las personas físicas, antes del tratamiento, se deberá realizar una evaluación de impacto.

  Whitehole debe de realizar una revisión continua de los tratamientos de datos personales realizados para poder valorar la necesidad de hacer una evaluación de impacto en cada caso.

  A título orientativo, la AEPD ha publicado un listado de tratamientos de datos personales que requieren de evaluación de impacto y son los siguientes:

  1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.
  2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o servicio o formar parte de un contrato.
  3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionadas con categorías especiales de datos.
5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.
6. Tratamiento que impliquen el uso de datos genéticos para cualquier fin.
7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.
8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.
9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.
10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.
11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b, c, d) del RGPD.

Whitehole valorará si aun realizándose alguno de los tratamientos descritos anteriormente, el mismo no entraña un alto riesgo para los derechos y libertades de los interesados y por ello no debe realizarse la evaluación de impacto. En este caso, se deberá documentar en el Registro de actividades del tratamiento las razones que han llevado a no realizar la evaluación de impacto.

Por otro lado, si la actividad de tratamiento cambia, será necesario que se realice una revisión y actualización de la evaluación de impacto.

A título orientativo, la AEPD también ha publicado un listado de tratamientos donde no sería necesario una evaluación de impacto y serían los siguientes:

1. Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.
2. Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en particular la AEPD, siempre y cuando una evaluación de impacto en protección de datos completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la evaluación de impacto.
3. Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizadas en interés público o en el ejercicio de poderes públicos

conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una evaluación de impacto, y siempre y cuando ya se haya realizado una evaluación de impacto completa.

4. Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.
5. Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.
6. Tratamientos realizados por comunidades y subcomunidades de propietarios tal y como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.
7. Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento de datos sensibles tales como los que se establecen en el artículo 9.1 del RGPD y no sea de aplicación el artículo 9.2 (d) de dicho Reglamento.

En el supuesto de que realizada la evaluación de impacto, se mostrara que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, deberá de consultarse a la autoridad de control antes del tratamiento. La respuesta de la consulta previa a la autoridad de control no tiene por objeto la obtención de un asesoramiento con relación a aspectos generales del cumplimiento de la normativa de protección de datos ni tampoco obtener la aprobación de tratamiento por parte de la autoridad de control, sino orientar al responsable con relación a aquellos riesgos que no hubiera sido capaz de identificar o mitigar suficientemente.

- **Delegado de Protección de Datos**

Whitehole ha designado un Delegado de Protección de Datos (DPO), atendiendo a lo dispuesto en el art. 37 del RGPD, al que ha dotado de funciones, responsabilidades y competencias profesionales específicas en materia de protección de datos personales, en consonancia con el principio de *Accountability* que persigue promover la responsabilidad y la rendición de cuentas en cuanto al cumplimiento del RGPD y la LOPDyGDD y respeto de los derechos de los titulares de datos personales.

El DPO reporta al más alto nivel jerárquico de la Gestora sin que pueda recibir ninguna instrucción para la consecución de las funciones asignadas, por ser independiente.

El DPO de Whitehole es accesible tanto para clientes, proveedores, empleados, y en general para para cualquier persona que interactúe con Whitehole, a través de la dirección de correo electrónico dpo@whitehole.es.

El art. 39 del RGPD establece que el DPO tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben conforme a la normativa vigente en materia de protección de datos;

b) supervisar el cumplimiento de lo dispuesto en la normativa vigente en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorias correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

4.2.6 Transferencias internacionales de datos personales. Las transferencias internaciones de datos personales suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

Podrán realizarse transferencias internacionales de datos, siempre que el tratamiento de datos observe lo dispuesto en el RGPD y la LOPDyGDD en los siguientes supuestos:

a) Transferencias basadas en una decisión de adecuación.

b) Transferencias mediante la aportación de garantías adecuadas.

c) Normas corporativas vinculantes

a) Transferencias basadas en una decisión de adecuación.

Cuando las entidades receptoras de los datos se encuentren en un país, un territorio o uno o varios sectores específicos de ese país u organización internacional que hayan sido declarados de nivel de protección adecuado por la Comisión Europea. En el siguiente link se encuentran los países y territorios que están declarados como adecuados por la Comisión:

https://www.aepd.es/es/preguntas-frecuentes/6-transferencias-internacionales-bcr-codigos-de-conducta/1-transferencias-internacionales/FAQ-0605-que-paises-se-consideran-con-un-nivel-adecuado-a-efectos-del-articulo-45-del-rgpd

b) Transferencias mediante la aportación de garantías adecuadas.

A falta de decisión de adecuación solo podrán transmitirse datos personales a un tercer país u organización internacional si se ofrecen garantías adecuadas y con la condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Las garantías adecuadas pueden ser aportadas a través de:

- un instrumento jurídicamente vinculante y exigible entre las autoridades y organismos públicos;
- normas corporativas vinculantes;
- cláusulas tipo de protección de datos adoptadas por la Comisión;
- cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión;
- códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a derechos de los interesados, o
- mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.

Excepciones:

A falta de decisión de adecuación y de garantías adecuadas, únicamente se podrán realizar transferencias internacionales de datos personales si se cumple alguna de las condiciones siguientes:

- La persona interesada haya dado explícitamente su consentimiento, después de haber sido informada de los posibles riesgos
- La transferencia sea necesaria para la ejecución de un contrato entre la persona interesada y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona interesada
- La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica
- La transferencia sea necesaria por razones importantes de interés público
- La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones
- La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento
- La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Si no resultase aplicable ninguna de estas excepciones, solo se podrá llevar a cabo una transferencia si no es repetitiva, afecta solo a un número limitado de personas interesadas, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades de la persona interesada, y el responsable del tratamiento evalúe todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofrezca garantías apropiadas con respecto a la protección de datos personales.

4.2.7 Formación en materia de protección de datos

Una de las funciones del Delegado de Protección de Datos recogida en el art. 39 del RGPD es la *"…formación del personal que participa en las operaciones de tratamiento".*

Whitehole impartirá formación general en materia de protección de datos a todos los empleados que traten datos personales. La formación se adaptará a las modificaciones legislativas que se puedan producir.

4.3 Tratamiento de la documentación original

Excepto en situaciones excepcionales, debidamente autorizadas, no se permite extraer la documentación original firmada por los clientes (aperturas de cuenta, documentos de apoyo a operaciones, contratos) de los archivos donde está almacenada. En caso de ser imprescindible su uso, se procederá a:

- Dejar fotocopia de la misma, informando de la fecha, motivo e identificación de la persona que ha extraído la documentación.
- Si se ha entregado a otro centro se remitirá la documentación original con acuse de recibo (físico o correo electrónico). Este será custodiado conjuntamente con la fotocopia realizada de la documentación.
- Al devolver la documentación también hay que solicitar un acuse de recibo o correo electrónico de la persona receptora de la misma. El departamento que devuelve la documentación archivará el acuse de recibo en el expediente que originó la petición de esta documentación o, en su defecto, se debe crear un archivo físico de estos comprobantes de todo el centro.
- Cuando se devuelva el original, deberá custodiarse de nuevo en el mismo archivo, adjuntando éste a la fotocopia y al acuse de recibo que dejamos en su día

5. SEGUIMIENTO Y CONTROL

Cualquier incidencia u observación relacionada con esta política general, deberá ser notificada inmediatamente al Departamento de Gestión de Riesgos o al Delegado de Protección de Datos (dpo@whitehole.es).

El cumplimiento de esta política está encargado al Delegado de Protección de Datos, quien supervisará el cumplimiento de las obligaciones en materia de protección de datos.

6. PENALIZACIONES

El incumplimiento de esta política y la vulneración de la seguridad de Whitehole están considerados en el Reglamento de Régimen Interno como faltas "graves" y "muy graves" respectivamente, y como tales, podrán dar lugar a la aplicación del régimen sancionador de Whitehole, y en su caso del Código Penal de España.

7. ANEXO I: DEFINICIONES

a) **Datos de carácter personal**: toda información sobre una persona física identificada o identificable (“el interesado”).

b) **Persona física identificable:** toda persona cuya identidad pueda determinarse, 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 propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

c) **Tratamiento de datos**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

d) **Responsable del tratamiento**: persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

e) **Interesado**: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado d) del presente artículo.

f) **Seudonimización**: tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales son se atribuyen a una persona física identificada o identificable.

g) **Anonimización**: el proceso de convertir los datos en una forma que no permita identificar a los individuos.

h) **Encargado del tratamiento**: la persona física o jurídica, autoridad pública, servicio o que trate datos personales por cuenta del responsable del tratamiento.

i) **Consentimiento del interesado**: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

j) **Cesión o comunicación de datos**: modalidad de tratamiento de datos personales por la que el responsable del tratamiento comunica los mismos, con consentimiento del interesado, a un tercero.

k) **Elaboración de perfiles:** toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

8. DOCUMENTACIÓN RELACIONADA

TABLA DE CONTROL DE CAMBIOS

Fecha	Nombre	Descripción de la revisión	Versión
Mayo 2024	Cumplimiento Normativo	Primera redacción	1