IAP
Asociación Internacional de Fiscales
Política de protección de datos
Septiembre de 2019

TABLA DE CONTENIDOS

El papel de la IAP

La Asociación Internacional de Fiscales (IAP)[1] es un organismo independiente, no gubernamental y apolítico; la única asociación profesional internacional para fiscales.

La IAP cuenta con más de 180 organizaciones miembros, entre ministerios públicos, asociaciones de fiscales y agencias de prevención del delito. Junto con los miembros privados, representa a más de 350.000 fiscales en más de 177 países y territorios en todo el mundo.

La IAP se propone fijar y mejorar las normas de conducta y ética profesional de los fiscales en todo el mundo; promover el Estado de derecho, la justicia, la imparcialidad y el respeto por los derechos humanos, y mejorar la cooperación internacional en la lucha contra el delito.

El Comité Ejecutivo es el órgano de gestión y administración de la IAP y está bajo la autoridad de la Asamblea general, órgano de gobierno de la Asociación. La Asociación elige un presidente, nueve (máximo) vicepresidentes y veintiún (máximo) miembros ordinarios adicionales que conforman el Comité ejecutivo. La composición del Comité ejecutivo representa las regiones del mundo donde la Asociación tiene miembros.

El Comité ejecutivo designa al Secretario general, director ejecutivo de la Asociación, y gestiona sus asuntos diarios, y al Consejero general, que desempeña la función de consejero legal y coordinador del programa profesional y de los proyectos de trabajo de la Asociación. El Director ejecutivo tiene a su cargo el reclutamiento de miembros y las relaciones con los miembros, el desarrollo y el funcionamiento de la red de la Asociación.

Sede del Secretariado de la IAP

El Secretariado de la IAP se encuentra en
Hartogstraat 13 2514 EP
La Haya
PAÍSES BAJOS

Reglamento europeo

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, comúnmente llamado **Reglamento general de protección de datos (GDPR)**.

El reglamento entró en vigor en mayo del 2018 y dejó sin efecto el reglamento general de protección de datos vigente bajo la Directiva europea de protección de datos.

El reglamento ha sido diseñado para proteger la privacidad de las personas. Confiere derechos individuales en relación con la privacidad de los datos personales, y establece responsabilidades para las personas físicas y jurídicas que conservan y procesan dicha información.

Habida cuenta de que la IAP procesa datos personales, está sujeta a ciertas obligaciones recogidas en el reglamento. Esta declaración explica cuáles son las obligaciones de la IAP y cómo se les dará cumplimiento. No aborda todas las situaciones posibles, de forma taxativa, ni proporciona asesoramiento legal.

¿Qué son los datos personales?

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o

[1] *Stichting* (fundación neerlandesa sin fines de lucro de la Tesorería de la IAP), establecida según ley neerlandesa.

determinables, también denominadas interesados. Los datos personales incluyen la siguiente información:

- Nombre;
- Domicilio;
- Número de identificación/pasaporte;
- Ingresos;
- Perfil cultural;
- Dirección IP (Protocolo de internet);
- Datos en poder de un hospital o médico (que identifican a la persona de forma unívoca para propósitos de salud)

Categorías especiales de datos personales

Las categorías especiales de datos personales son datos relacionados con

- el origen étnico o racial;
- las opiniones políticas;
- las convicciones religiosas o filosóficas;
- la afiliación sindical;
- 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 las orientaciones sexuales de una persona física.

Según el GDPR, está prohibido tratar categorías especiales de datos personales a menos que se cumpla con alguno de los supuestos del Artículo 9. Las categorías especiales de datos conservadas por la IAP, si las hubiera, probablemente sean limitadas.

Si se propusiera el tratamiento de categorías especiales de datos personales, se deberá cumplir con las condiciones necesarias antes de proceder al tratamiento.

¿Qué es el tratamiento?

El tratamiento de datos personales es una operación o conjunto de operaciones con los datos, de forma automatizada o no, que incluye recopilación, registro, organización, estructuración, conservación, adaptación o alteración, extracción, consulta, uso, divulgación mediante transferencia, difusión o de otro modo, alineación o combinación, restricción, supresión o eliminación.

Durante el tratamiento, los datos personales pueden pasar por distintas empresas u organizaciones. En este proceso intervienen dos entidades principales

- El responsable del tratamiento de datos (controlador);
- El encargado del tratamiento de datos (procesador);

¿Quién es el responsable del tratamiento de datos?

El responsable es la organización que, de forma individual o en conjunto con otras, determina la finalidad y aplica las medidas para el tratamiento de datos personales. La IAP es el responsable del tratamiento de datos. Tiene su sede en la Haya, Países Bajos, Unión Europea.

¿Quién es el encargado del tratamiento de datos?

El encargado del tratamiento es una persona física o jurídica, autoridad gubernamental, agencia u órgano que procesa los datos personales en nombre del responsable. Parte del trabajo de la IAP lo realizan encargados de tratamiento externos. Estos encargados deben actuar según las instrucciones de la IAP y

estarán sujetos a las obligaciones relativas al uso de datos personales inscritas en este reglamento.

Principios del GDPR

Durante el tratamiento de datos personales se deben cumplir los siguientes principios de protección de datos:

a) Los datos serán tratados de manera lícita y leal;
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados;
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan;
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales;
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Licitud del tratamiento

No se procesarán datos personales a menos que sea lícito hacerlo. Los fundamentos de licitud del tratamiento están dispuestos en el Artículo 6 del GDPR. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) Consentimiento: el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) Contrato: el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) Obligación legal: el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) Interés vital: el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) Interés legítimo: el tratamiento es necesario para la satisfacción de intereses comerciales legítimos perseguidos por la organización;
f) Misión de interés público: el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de las funciones oficiales del organismo, y la misión o función tienen un evidente fundamento jurídico;

La IAP utiliza múltiples plataformas incluidos los sistemas de gestión de base de datos, sitios web, sistemas de registro de eventos, redes exclusivas para miembros y sistemas manuales de mantenimiento y tratamiento de datos.

En general, la IAP recopila y usa información personal sobre la base de un interés jurídico legítimo. Cuando, por ejemplo, un miembro solicita servicios o productos de la IAP, la IAP tiene el interés legítimo de la organización para usar los datos personales del solicitante a fin de responder a la solicitud, y el uso que haga la IAP de esos datos y con ese fin no comporta un perjuicio para el miembro. En algunos casos, la IAP deberá obtener el consentimiento del interesado antes de usar la información personal.

Solicitud de acceso a datos personales

Toda persona cuya información personal esté siendo usada por la IAP tiene el derecho a saber

- Con qué finalidad se están tratando los datos;
- Qué tipo de información personal está siendo tratada;
- Los terceros, en su caso, a los que se hayan divulgado los datos;

- El plazo durante el cual la IAP conservará esos datos.

El interesado puede solicitar información sobre los datos personales suyos que se hayan recopilado mediante una **Solicitud de acceso**. La persona tiene derecho a acceder únicamente a sus propios datos personales, no a los de un tercero.

La persona que solicite dicho acceso deberá proporcionar al Secretariado de la IAP la información necesaria para que el Secretariado pueda identificar al interesado de forma unívoca y pueda localizar los datos o la información personal correspondiente.

Si el pedido de datos personales fuera manifiestamente infundado o excesivo, la IAP podrá exigir el pago de una tasa razonable u objetar la solicitud.

Derecho a la información

El derecho de acceso otorga al interesado el derecho a obtener una copia de sus datos personales e información complementaria que, en líneas generales, se corresponde con la información incluida en la **Declaración de privacidad de la IAP** publicada en el sitio web de la IAP.

Derecho de rectificación, supresión o restricción al tratamiento

Según el GDPR, los interesados tienen el derecho a que cualquier dato personal incorrecto sea rectificado. El interesado tiene derecho a solicitar una restricción al tratamiento de sus datos personales, mientras la objeción respecto de la exactitud de los datos y la verificación por parte de la IAP estén en curso. La IAP puede negarse a dar curso a la solicitud de rectificación si es manifiestamente infundada o excesiva.

Conservación

No se deberán conservar datos personales por un período superior al necesario para la finalidad y la conservación estará sujeta a revisiones periódicas a cargo del Secretariado.

Restricciones al ejercicio del derecho de acceso a los datos de un interesado

El responsable puede restringir, total o parcialmente, el derecho de acceso a los datos de un interesado en ciertos supuestos. Las restricciones se encuentran listadas en el Capítulo III del GDPR.
Si el responsable decidiera restringir el ejercicio del derecho de acceso a los datos de un interesado, deberá generar y mantener un registro escrito con los fundamentos fácticos y jurídicos de tal decisión. Este registro se pondrá a disposición del órgano supervisor.
El interesado podrá presentar una reclamación ante el órgano supervisor por habérsele restringido el derecho de acceso a los datos.

Registro de actividades de tratamiento de datos personales

Se debe llevar un registro de las actividades de tratamiento de cada una de las categorías de datos personales, según lo dispuesto en el GDPR. El registro debe mantenerse actualizado y dar cuenta de cualquier modificación en las actividades de tratamiento, y ser puesto a disposición del órgano de supervisión siempre que éste solicite su inspección.

Transferencia de datos a terceros países y organismos internacionales

El GDPR obliga principalmente a los responsables y encargados del tratamiento de datos ubicados en el Espacio Económico Europeo (EEE) con algunas excepciones.

Los países dentro del EEE son Estados miembros de la UE y Estados miembros de la Asociación Europea de Libre Comercio (AELC). Los Estados miembros de la UE son Austria, Bélgica, Bulgaria, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Irlanda, Italia, Letonia,

Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Rumanía, Eslovaquia, Eslovenia, España, Suecia y Reino Unido. Los estados de la AELC son Islandia, Noruega y Liechtenstein.

El GDPR restringe la transferencia de datos personales fuera de la EEE o la tutela del GDPR, a menos que los derechos del interesado en relación con los datos personales estén protegidos de otro modo o se aplique alguna de las escasas excepciones.

El trabajo de la IAP, en ocasiones, exige que se transfieran datos personales a un país fuera de la EEE. Esto se denomina **transferencia restringida** en el marco del GDPR. Es posible realizar una transferencia restringida cuando

La transferencia restringida se encuentra amparada por una **decisión de adecuación** de la Comisión Europea. Es decir, cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección de los derechos y libertades del interesado adecuado.

Las decisiones de adecuación adoptadas previo al GDPR permanecerán vigentes a menos que una decisión de la Comisión disponga lo contrario. Se puede acceder a lista actualizada de países con dictamen de adecuación en el sitio web de protección de datos de la Comisión Europea.

En ausencia de una decisión de adecuación de la Comisión respecto de un tercer país, un territorio o sector específico de un tercer país, la transferencia se realizará si se cumple con las **garantías adecuadas**, incluidas en el GDPR. Estas garantías implican que las partes involucradas en la transferencia tengan normas vinculantes para la protección de los datos personales y otros derechos y libertades fundamentales.

En ausencia de una decisión de adecuación o de garantías adecuadas, la transferencia se realizará si se aplica alguna de las excepciones enumeradas en el Artículo 49 del GDPR. Estas son **excepciones a la prohibición general cuando se trate de necesidades específicas** y siempre que el interesado dé su consentimiento explícito a la transferencia de datos, tras haber sido informado de los riesgos potenciales de dichas transferencias para el interesado dada la ausencia de una decisión de adecuación o de garantías adecuadas.

Violación de la seguridad de los datos personales

Toda violación de la seguridad de los datos personales debe ser informada al Secretariado de la IAP, sin dilación. Esto incluye violaciones constatadas por parte de los responsables del tratamiento de datos de la IAP.

Las violaciones de la seguridad de los datos personales se pueden definir, en general, como incidentes de seguridad que han afectado la confidencialidad, integridad o la disponibilidad de los datos personales. Es decir, violación de la seguridad de los datos personales se define como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración de datos personales, o la comunicación o acceso no autorizados a dichos datos; o la imposibilidad de acceder a los datos por haber sido encriptados por *ransomware*, o perdidos o destruidos accidentalmente.

Tan pronto como el Secretario General tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, debe, sin dilación indebida y a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales al órgano supervisor. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación.

La notificación debe describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible

- las categorías y el número aproximado de interesados afectados;
- las categorías y el número aproximado de registros de datos personales afectados;

- el punto de contacto en el que pueda obtenerse más información;
- una descripción de las posibles consecuencias de la violación de la seguridad de los datos personales; y
- una descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si la violación de la seguridad pudiera constituir un riesgo para los derechos y las libertades de las personas físicas, el Secretariado notificará a los involucrados directamente y sin dilación indebida.

Obligaciones del personal de la IAP

El personal de la IAP debe estar familiarizado con el contenido de la **Política de protección de datos de la IAP**, la **Declaración de privacidad de la IAP** y los principios generales de protección de datos. El personal debe saber que está obligado a conservar los datos personales de forma segura, exacta y actualizada, y que podrá procesar los datos personales sólo para el fin con el cual se recopilaron y en cumplimiento de los principios de protección de datos.

El personal de la IAP debe poner especial atención al extraer datos personales que pertenezcan a la IAP de las instalaciones comerciales de la IAP; debe asegurarse de que los datos electrónicos estén almacenados en hardware encriptado o en una memoria USB encriptada y que los archivos en papel estén protegidos en todo momento. Al transferir datos personales electrónicos a otras personas deben asegurarse de que los métodos empleados sean seguros y que cumplan con el GDPR.

El personal de la IAP debe seguir las instrucciones relativas al almacenamiento de datos personales dentro de la red de la IAP.

Órgano supervisor

El Secretariado de la IAP tiene sede en La Haya y está sujeto a la legislación nacional aplicable en materia de protección de datos de Países Bajos.

El órgano supervisor de Países Bajos es

Autoriteit Persoonsgegevens
Bezuidenhoutseweg 30
PO Box 93374, 2509 AJ Den Haag
Sitio web: https://autoriteitpersoonsgegevens.nl/en