



Ibermática

**Política Privacidad y
Protección de Datos
Personales**

SGQ-RGPD-POLPII



Control de la documentación

La última versión de este documento está disponible en la Intranet. Si utiliza el documento impreso (documento no controlado) **asegúrese que es la versión vigente y que está completo** consultando la lista de documentos vigentes del Sistema de Gestión de la Calidad integrado publicada en la Intranet

Participantes

Responsabilidad	Nombre / función
<i>Propietario:</i>	Ibermática S.A.
<i>Desarrollado por:</i>	Jesús Martín González / Responsable de Calidad, Seguridad y Continuidad. Delegado de Protección de Datos
<i>Revisado por:</i>	César Saiz Sanz / Asesoría Jurídica Víctor Merino Fernández-Pellón / Asesoría Jurídica
<i>Aprobado por:</i>	Jesús Martín González / Responsable de Calidad, Seguridad y Continuidad. Delegado de Protección de Datos

Memoria

Versión	Fecha aprobación	Cambio producido
01	31/12/2019	Primera versión.

Contenidos

1.	Introducción.....	1
1.1.	Alcance.....	1
1.2.	Objeto.....	2
1.3.	Contenido.....	2
1.4.	Documentos relacionados.....	2
1.5.	Glosario (definiciones).....	3
2.	Delegado de Protección de Datos de Ibermática (DPD)	5
3.	Principios generales de la protección de datos.....	6
3.1.	Principio de LEALTAD	6
3.2.	Principio de PROPORCIONALIDAD.....	6
3.3.	Principio de LICITUD.....	6
3.4.	Principio de TRANSPARENCIA	6
3.5.	Principio de FINALIDAD y LIMITACIÓN DE FINALIDAD.....	6
3.6.	Principio de COMPATIBILIDAD.....	6
3.7.	Principio de MINIMIZACIÓN DE DATOS.....	6
3.8.	Principio de EXACTITUD.....	6
3.9.	Principio de LIMITACIÓN DEL PLAZO DE CONSERVACIÓN.....	6
3.10.	Principio de INTEGRIDAD, CONFIDENCIALIDAD y SEGURIDAD.....	7
3.11.	Principio de PROTECCION DE DATOS DESDE EL DISEÑO y POR DEFECTO	7
3.12.	Principio de RESPONSABILIDAD PROACTIVA o DILIGENCIA DEBIDA.....	7
4.	Condiciones para el consentimiento.....	8
5.	Categorías especiales de datos.....	9
6.	Tratamiento de datos personales.....	10
6.1.	Tratamiento de datos personales relativos a condenas e infracciones penales	10
6.2.	Información a proporcionar a los interesados sobre el tratamiento de sus datos	10
7.	Ejercicio de Derechos	12
7.1.	Derecho de ACCESO	12
7.2.	Derecho de RECTIFICACIÓN.....	12
7.3.	Derecho de SUPRESIÓN (<<derecho al olvido>>)	12
7.4.	Derecho a la LIMITACIÓN DEL TRATAMIENTO	13
7.5.	Derecho a la PORTABILIDAD DE LOS DATOS.....	13
7.6.	Derecho de OPOSICIÓN	13
7.7.	Derecho a NO SER OBJETO DE UNA DECISIÓN INDIVIDUAL AUTOMATIZADA.....	13
8.	Prestación de servicios por terceros.....	14
9.	Registro de Actividades de Tratamiento (RAT).....	15
10.	Medidas de seguridad.....	16
10.1.	Deber de secreto.....	17
11.	Transferencias internacionales de datos.....	18
12.	Infracciones y sanciones previstas en la normativa vigente	20
12.1.	Actuaciones en relación con la Agencia Española de Protección de Datos	20
12.2.	Obligaciones del personal.....	20
12.3.	Consultas.....	20



13.	Controles para el adecuado cumplimiento de esta política	21
14.	Revisión.....	22
15.	Validez y gestión documental.....	23

1. Introducción

La Constitución Española, en su artículo 18 garantiza el derecho al honor, la intimidad personal y familiar y a la propia imagen. En particular, en su apartado cuarto, establece la necesidad de proteger estos derechos fundamentales, dentro del ámbito relacionado con el uso de la informática. De esta manera, el artículo 18.4 de nuestra Constitución dispone:

“La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”

Como consecuencia de este mandato y para desarrollar el contenido del mismo, se promulgó la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal (LO 5/1992, de 29 de octubre), conocida como LORTAD.

Posteriormente, se promulgó en el marco de la Unión Europea la Directiva 95/46/CEE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los datos.

En cumplimiento de esta Directiva, España promulgó la Ley Orgánica de Protección de Datos de Carácter Personal (LO 15/1999, de 13 de diciembre), en adelante LOPD, y que supuso la transposición de la Directiva 95/46/CE al derecho interno de nuestro país y, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

No obstante, para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión Europea, era necesario un reglamento que proporcionase seguridad jurídica y transparencia a los operadores económicos, y ofreciese a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros.

Por ello, fue aprobado y entró en vigor el 25 de mayo de 2016, 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).

En la actualidad, el vigente Reglamento General de Protección de Datos de la Unión Europea (RGPD) ha derogado la Directiva 95/46/CEE y es plenamente aplicable para todo el territorio de la Unión Europea de forma directa.

En España, se han desarrollado algunos aspectos y establecido otros en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, conocida como LOPDGDD. El objeto es adaptar el Derecho interno español al Reglamento General de Protección de Datos.

El citado RGPD, en su artículo 24, establece como una obligación de responsabilidad proactiva del responsable del tratamiento, la necesidad de establecer las oportunas políticas de protección de datos, a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento.

Una de las obligaciones básicas para el responsable del tratamiento es la formación del personal que participa en las operaciones de tratamiento de los datos y la concienciación de dicho personal en la importancia y necesidad del cumplimiento de la normativa.

Con base en lo anterior y, consciente de la importancia de que el personal conozca la normativa vigente sobre protección de datos, se ha elaborado la presente normativa interna en materia de privacidad y protección de datos de obligado cumplimiento para todos los empleados de Ibermática.

1.1. Alcance

Esta política es de aplicación a Ibermática S.A. y a todas las sociedades del Grupo Ibermática (en adelante Ibermática).



La presente política es de obligado cumplimiento para todas las sociedades de Ibermática, los departamentos que las componen y sus empleados y afecta tanto a datos personales tratados por medios electrónicos como en soporte papel.

1.2. Objeto

Constituye el objeto de la presente normativa proporcionar formación e información a los empleados de Ibermática en materia de privacidad y protección de datos, a tener en cuenta y respetar en desarrollo y el ejercicio de sus funciones.

Esta normativa está dirigida a todas las unidades de negocio que componen las distintas sociedades de Ibermática y, en particular, a aquellas que intervienen en el tratamiento de datos de carácter personal, así como a los directivos de estas unidades, centros de responsabilidad, al personal autorizado para acceder e informar de los mismos y para el personal de desarrollo.

1.3. Contenido

Además de este capítulo introductorio, el presente documento incluye:

- Delegado de Protección de Datos de Ibermática (DPD).
- Principios generales de la protección de datos.
- Condiciones para el consentimiento.
- Categorías especiales de datos.
- Tratamiento de datos personales.
- Ejercicio de derechos.
- Prestación de servicios por terceros.
- Registro de Actividades de Tratamiento (RAT).
- Medidas de seguridad.
- Transferencias internacionales de datos.
- Infracciones y sanciones previstas en la normativa vigente.
- Controles para el adecuado cumplimiento de esta política.
- Revisión.
- Validez y gestión documental.

1.4. Documentos relacionados

- [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.
- [Código de Protección de Datos Personales \(BOE\)](#).
- [Ley Orgánica 3/2018](#), de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Informes y recomendaciones de la Agencia Española de Protección de Datos y del Grupo de trabajo del artículo 29 (WP29).
- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información
- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO/IEC 29184:2020 Information technology -- Online privacy notices and consent
- [Código de buenas prácticas para la protección de datos personales](#) (en Ibermática) v01

1.5. Glosario (definiciones)

A efectos de la presente normativa y del RGPD se entenderá por:

Datos personales	toda información sobre una persona física identificada o identificable («el/a interesado/a»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante su imagen, voz, 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;
Tratamiento	cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, 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;
Limitación del tratamiento	el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;
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;
Seudonimización	el 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 no se atribuyan a una persona física identificada o identificable;
Fichero	todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
Responsable del tratamiento o Responsable	la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;
Encargado del tratamiento o Encargado	la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;
Destinatario	la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;
Tercero	persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;
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;
Violación de la seguridad de los	toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de



datos personales	otra forma, o la comunicación o acceso no autorizados a dichos datos;
Datos genéticos	datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;
Datos biométricos	datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;
Datos relativos a la salud	datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;
Empresa	persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;
Grupo empresarial	grupo constituido por una empresa que ejerce el control y sus empresa controladas;
Normas corporativas vinculantes	las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;
Autoridad de control	la autoridad pública independiente establecida por un Estado miembro con la responsabilidad de supervisar la aplicación del RGPD, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión. En España es la Agencia Española de Protección de Datos (AEPD).
Autoridad de control interesada	la autoridad de control a la que afecta el tratamiento de datos personales debido a que: a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c) se ha presentado una reclamación ante esa autoridad de control;
Tratamiento transfronterizo	a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;
Servicio de la sociedad de la información	todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo;
Organización internacional	una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

2. Delegado de Protección de Datos de Ibermática (DPD)

Ibermática dispone de un delegado de protección de datos que, entre otras funciones, tiene las siguientes:

- informar y asesorar a los empleados que tratan datos personales de las obligaciones que les incumben en virtud de la normativa vigente en protección de datos;
- supervisar el cumplimiento de lo dispuesto en la normativa vigente en protección de datos y de las políticas de protección de datos de Ibermática;
- la asignación de responsabilidades, concienciación y formación del personal que participa en las operaciones de tratamiento;
- la realización de las auditorías correspondientes (en base a la norma internacional ISO 27701, el RGPD y la LOPDGDD);
- ofrecer asesoramiento acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad;
- cooperar con la autoridad de control, y en concreto, con la Agencia Española de Protección de Datos;
- actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar las consultas que proceda a dicha autoridad, en su caso, sobre cualquier otro asunto.

Los datos del delegado de protección de datos de Ibermática son:

- Jesús Martín González
- Dirección: Calle Campezo, 1, bloque 4-5, Parque Empresarial Las Mercedes, 28022, Madrid
- Tlf.: +34 913 849 100
- E-mail: dpd@ibermatica.com

3. Principios generales de la protección de datos

3.1. Principio de LEALTAD

Implica el cumplimiento de todas las normas de Derecho generales y/o sectoriales aplicables al tratamiento, así como las políticas y normas de Ibermática.

3.2. Principio de PROPORCIONALIDAD

Implica que el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio/proporcionalidad con otros derechos fundamentales.

3.3. Principio de LICITUD

Implica que cualquier tratamiento tendrá una base jurídica de entre las siguientes:

- Consentimiento del interesado para el tratamiento de sus datos personales para uno o varios fines específicos;
- Ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- Cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- Protección de los intereses vitales del interesado o de otra persona física;
- Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- Satisfacción de intereses legítimos perseguidos por Ibermática o por un tercero directamente relacionado con Ibermática, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.

3.4. Principio de TRANSPARENCIA

Implica que el interesado/a será informado/a del alcance del tratamiento de forma leal, inequívoca, específica y expresa.

3.5. Principio de FINALIDAD y LIMITACIÓN DE FINALIDAD

Implica que el tratamiento de los datos siempre se llevará a cabo con fines explícitos, legítimos y específicos.

3.6. Principio de COMPATIBILIDAD

Implica que no se llevarán a cabo tratamientos de datos con fines incompatibles con aquellos que motivaron la recogida de los datos. No se considerarán en todo caso incompatibles los fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

3.7. Principio de MINIMIZACIÓN DE DATOS

Implica que los datos sometidos a tratamiento serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados y a los mínimos datos posibles.

3.8. Principio de EXACTITUD

Implica que se someterán a tratamiento datos exactos y, si fuera necesario, actualizados; adoptando 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.

3.9. Principio de LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

Implica que los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento para los que fueron recogidos los datos personales.



3.10. Principio de INTEGRIDAD, CONFIDENCIALIDAD y SEGURIDAD

Implica que los datos personales serán 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.

3.11. Principio de PROTECCION DE DATOS DESDE EL DISEÑO y POR DEFECTO

Implica la reducción al máximo del tratamiento de datos personales, en relación con

- la cantidad de datos personales recogidos;
- la extensión de su tratamiento;
- su plazo de conservación; y
- su accesibilidad.

3.12. Principio de RESPONSABILIDAD PROACTIVA o DILIGENCIA DEBIDA

Implica que el responsable y el encargado del tratamiento deben cumplir con los principios antedichos y ser capaces de demostrarlo, ante cualquier tercero que en aplicación de la normativa vigente pudiera requerir su cumplimiento.

4. Condiciones para el consentimiento

Cuando el tratamiento se base en el consentimiento del/a interesado/a, el responsable deberá ser capaz de demostrar que aquel/la consintió el tratamiento de sus datos personales.

Si el consentimiento del/a interesado/a se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo, evitando la obtención de consentimientos no admisibles (tácitos ...).

No será vinculante ninguna parte de la declaración que constituya infracción de lo dispuesto anteriormente y, además, el/a interesado/a tendrá derecho a retirar su consentimiento en cualquier momento.

La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada.

Antes de dar su consentimiento, el/a interesado/a será informado/a de ello.

Además, deberá ser tan fácil retirar el consentimiento como darlo.

Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato o prestación de servicio.

5. Categorías especiales de datos

Queda prohibido el tratamiento de 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.

Lo anterior no será de aplicación cuando concurra una de las circunstancias siguientes:

- el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando alguna norma de Derecho establezca que la prohibición mencionada en el apartado anterior no puede ser levantada por el/a interesado/a;
- el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del/a interesado/a en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
- el tratamiento es necesario para proteger intereses vitales del/a interesado/a o de otra persona física, en el supuesto de que el/a interesado/a no esté capacitado/a, física o jurídicamente, para dar su consentimiento;
- el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, 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;
- el tratamiento se refiere a datos personales que el/a interesado/a ha hecho manifiestamente públicos;
- el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
- el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del/a interesado/a;
- el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del/a trabajador/a, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de otras condiciones y garantías que se contemplen en el RGPD;
- el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, 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 que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;
- el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1 del RGPD, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del/a interesado/a.

6. Tratamiento de datos personales

6.1. Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.

Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

6.2. Información a proporcionar a los interesados sobre el tratamiento de sus datos

Cuando los datos se obtengan del interesado/a directamente, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

- la identidad y los datos de contacto del responsable;
- los datos de contacto del delegado de protección de datos;
- los fines del tratamiento a que se destinan los datos personales;
- la base jurídica del tratamiento;
- cuando el tratamiento se base en el interés legítimo, los intereses legítimos del responsable o de un tercero;
- los destinatarios o las categorías de destinatarios de los datos personales;
- la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en su caso, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado;
- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
- cuando el tratamiento esté basado en el consentimiento, la existencia del 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;
- el derecho a presentar una reclamación ante una autoridad de control;
- si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el/a interesado/a está obligado/a a facilitar los datos personales y está informado/a de las posibles consecuencias de que no facilitar tales datos;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el/a interesado/a;
- si se proyecta el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al/a interesado/a, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente.

Cuando los datos personales no se hayan obtenidos del/a interesado/a, el responsable del tratamiento le facilitará la siguiente información, además de toda la indicada en el apartado anterior:

- las categorías de datos personales de que se trate;
- la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

La información indicada en los apartados anteriores se proporcionará al/a interesado/a:

- dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
- si los datos personales han de utilizarse para comunicación con el/a interesado/a, a más tardar en el momento de la primera comunicación a dicho/a interesado/a; o
- si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.



No obstante, lo anterior no será de aplicación cuando y en la medida en que:

- el/a interesado/a ya disponga de la información;
- la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1 del RGPD, o en la medida en que la obligación mencionada en el apartado 1 del citado artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
- la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado; o
- cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

7. Ejercicio de Derechos

Los siguientes derechos están garantizados y gestionados en la medida en que sean ejercitados por los/as interesados/as, teniendo en cuenta para ello, su alcance, particularidades y limitaciones.

La atención y gestión de estos derechos se llevará a cabo según el procedimiento de ejercicio de derechos, a través de la dirección de email: arco@ibermatica.com, donde por tanto, cualquier empleado deberá notificar la existencia y recepción de cualquier tipo de comunicación recibida en Ibermática por terceros interesado/as.

Igualmente, a través de las comunicaciones vía internet, donde se sugiere a los terceros interesados/as el uso de dicha dirección de correo electrónico para el ejercicio de los posibles derechos.

Lo/as interesado/as serán informado/as de los siguientes derechos, que, además, serán atendidos y gestionados en la medida en que sean objeto de ejercicio:

7.1. Derecho de ACCESO

Proporciona al/a interesado/a el derecho a obtener del 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 y a la siguiente información:

- los fines del tratamiento;
- las categorías de datos personales de que se trate;
- los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
- de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al/a interesado/a, o a oponerse a dicho tratamiento;
- el derecho a presentar una reclamación ante una autoridad de control;
- cuando los datos personales no se hayan obtenido del/a interesado/a, cualquier información disponible sobre su origen;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el/a interesado/a. Cuando se transfieran datos personales a un tercer país o a una organización internacional, las garantías adecuadas en virtud del artículo 46 del RGPD relativas a la transferencia.

7.2. Derecho de RECTIFICACIÓN

Proporciona al/a interesado/a el derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan y/o a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

7.3. Derecho de SUPRESIÓN (<<derecho al olvido>>)

Proporciona al/a interesado/a el derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concorra 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/a interesado/a retire el consentimiento en que se basa el tratamiento, y este no se base en otro fundamento jurídico;



- el/a interesado/a se oponga al tratamiento por motivos relacionados con su situación particular, y no prevalezcan otros motivos legítimos para el tratamiento, o el/a interesado/a se oponga al tratamiento con fines de mercadotecnia (publicidad);
- los datos personales hayan sido tratados ilícitamente;
- los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho que se aplique al responsable del tratamiento;
- los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información cuando el/a interesado/a era menor.

7.4. Derecho a la LIMITACIÓN DEL TRATAMIENTO

Proporciona al/a interesado/a el derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- el/a interesado/a 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/a interesado/a 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/a interesado/a los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
- el/a interesado/a se haya opuesto al tratamiento basado en motivos relacionados con su situación particular, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del/a interesado/a.

7.5. Derecho a la PORTABILIDAD DE LOS DATOS

Proporciona al/a interesado/a el 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 en un contrato, y
- el tratamiento se efectúe por medios automatizados.

7.6. Derecho de OPOSICIÓN

Proporciona al/a interesado/a el 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 cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos del responsable o en la satisfacción del interés legítimo del responsable, incluida la elaboración de perfiles.

El responsable del tratamiento 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/a interesado/a, o para la formulación, el ejercicio o la defensa de reclamaciones.

Este derecho también proporcionará al/a interesado/a el derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan con fines de mercadotecnia (publicidad), incluida la elaboración de perfiles relacionada con este fin.

Además, cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1 del RGPD, el/a interesado/a tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

7.7. Derecho a NO SER OBJETO DE UNA DECISIÓN INDIVIDUAL AUTOMATIZADA

Proporciona al/a interesado/a el derecho a no ser objeto de una decisión individual automatizada, incluida la elaboración de perfiles basada únicamente en el tratamiento automatizado, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.



8. Prestación de servicios por terceros

Cuando se vaya a realizar un tratamiento por cuenta de Ibermática se elegirá un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos de los/as interesados/as.

Se prohibirá al encargado del tratamiento recurrir a otro encargado sin la autorización previa por escrito, específica o general, del responsable, informándole de que, en caso de autorización deberá informar al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

Siempre se regulará por escrito la relación con los terceros encargados del tratamiento, mediante un contrato de encargo de tratamiento (Acuerdo de Encargo de Tratamiento), que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Dicho contrato estipulará, en particular, que el encargado:

- tratará los datos personales únicamente siguiendo instrucciones documentadas de Ibermática, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
- garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
- tomará todas las medidas necesarias en materia de seguridad, de conformidad con el artículo 32 del RGPD;
- respetará las condiciones indicadas por el responsable para recurrir a otro encargado del tratamiento;
- asistirá a Ibermática, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los/as interesados/as;
- ayudará a Ibermática a garantizar el cumplimiento de las obligaciones de seguridad, incluida la notificación de brechas o violaciones de seguridad a la Autoridad de Control, así como a los/as interesados/as, y ayudará a la realización de una evaluación de impacto en protección de datos, incluida la consulta previa a la AEPD, todo ello, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
- a elección de Ibermática, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho aplicable;
- pondrá a disposición de Ibermática toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas anteriormente establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

El contrato de encargo de tratamiento descrito, será proporcionado al personal que lo necesite a través de Asesoría Jurídica (Asesoria_juridica@ibermatica.com) de Ibermática.

9. Registro de Actividades de Tratamiento (RAT)

Ibermática llevará a un Registro de Actividades de Tratamiento (RAT) que contendrá la siguiente información:

- nombre y datos de contacto de Ibermática como entidad responsable y, en su caso, si los hubiera, de terceros corresponsables y del representante del responsable;
- nombre y datos de contacto del delegado de protección de datos;
- los fines del tratamiento;
- una descripción de las categorías de interesados;
- una descripción de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- los destinatarios en terceros países u organizaciones internacionales, esto es, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en su caso, la documentación de garantías adecuadas;
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad de la información.

10. Medidas de seguridad

Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre 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 otro perjuicio económico o social significativo para la persona física en cuestión.

Los datos serán 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 («integridad y confidencialidad»).

Cada responsable del tratamiento de actividades, y el encargado del tratamiento, deberán llevar un registro de todas las categorías de actividades de tratamiento de datos personales efectuadas por Ibermática. Dicho registro deberá contener una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30 del Reglamento General de Protección de Datos (RGPD).

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo teniéndose en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de 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.

El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, deberá acompañarse una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

Igualmente, el responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en



cuenta las circunstancias de tal violación, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido. Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales.

Si Ibermática debe llevar a cabo una evaluación de impacto en protección de datos, como responsable del tratamiento tendrá en cuenta las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

10.1. Deber de secreto

Un principio básico y personal para toda persona que intervenga en el tratamiento de datos personales es su obligación de secreto profesional respecto de dichos datos y su deber de guardarlos, subsistiendo dichas obligaciones aún después de finalizar sus relaciones con el responsable del tratamiento o, en su caso, con el encargado del tratamiento.

Por lo tanto, no debe revelarse bajo ningún concepto información de carácter personal a terceras personas distintas del/a interesado/a, aun cuando exista vínculo de parentesco (ni si quiera verbalmente), salvo que se establezca por Ley o por expresa autorización del interesado.

Esta obligación se alinea con la normativa laboral y con los acuerdos que los empleados de Ibermática asumen cuando formalizan su relación laboral.

11. Transferencias internacionales de datos

Cualquier área de Ibermática que necesite transferir datos de carácter personal fuera del Espacio Económico Europeo, lo consultará previamente con Asesoría Jurídica ([Asesoría jurídica@ibermatica.com](mailto:Asesoria_juridica@ibermatica.com)) de Ibermática.

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, tanto Ibermática como los responsables y el encargados del tratamiento que intervengan en la transferencia, cumplen las condiciones establecidas en el RGPD, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

Las reglas a tener en cuenta se indican a continuación.

Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido (mediante acto de ejecución o Decisión adecuada) 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 adecuado. Dicha transferencia no requerirá ninguna autorización específica.

A falta del acto y/o Decisión de la Comisión, Ibermática solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Las garantías adecuadas con arreglo al RGPD podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

- un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
- normas corporativas vinculantes aprobadas por la Autoridad de Control de conformidad con el mecanismo de coherencia del artículo 63 del RGPD;
- cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2 del RGPD;
- cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2 del RGPD;
- un código de conducta aprobado con arreglo al artículo 40, 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 los interesados; o
- un mecanismo de certificación aprobado con arreglo al artículo 42 del RGPD, 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 los interesados.

Además, Ibermática podrá aportar sus propias garantías adecuadas, en cuyo caso será precisa y obligatoria la autorización de la Agencia Española de Protección de Datos, mediante:

- cláusulas contractuales entre el responsable el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o
- disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

En ausencia de un acto y/o Decisión de adecuación de la Comisión, o de las garantías adecuadas, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará por Ibermática si se cumple alguna de las condiciones siguientes:

- el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;
- la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;



- la transferencia es 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 es necesaria por razones importantes de interés público;
- la transferencia es necesaria para la formulación, el ejercicio o la defensa de reclamaciones;
- la transferencia es necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;
- la transferencia se realiza 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.

Cuando una transferencia no pueda basarse en un acto o Decisión de la Comisión o en las garantías adecuadas, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas de las mencionadas con anterioridad, solo se podrá llevar a cabo la transferencia internacional por Ibermática si se cumplen todos los siguientes requisitos:

- si no es repetitiva;
- si afecta solo a un número limitado de interesados;
- si es necesaria a los fines de intereses legítimos imperiosos perseguidos por Ibermática sobre los que no prevalezcan los intereses o derechos y libertades del interesado;
- si se han evaluado todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, Ibermática ofrece garantías apropiadas con respecto a la protección de datos personales.

En estos casos Ibermática deberá informar a la autoridad de control de la transferencia y, además de la información a que hacen referencia los artículos 13 y 14 del RGPD, Ibermática informará al interesado de la transferencia de los intereses legítimos imperiosos perseguidos.

Ibermática documentará en sus registros de actividad la evaluación y las garantías apropiadas referidas en este punto.

12. Infracciones y sanciones previstas en la normativa vigente

Las infracciones de lo establecido en el RGPD se sancionarán por la Autoridad de Control, entre otras sanciones, con multas administrativas que, en función del tipo de infracción podrán oscilar entre 10.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, y multas administrativas de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

12.1. Actuaciones en relación con la Agencia Española de Protección de Datos

Corresponde al Delegado de Protección de Datos de Ibermática la interlocución y el mantenimiento de las relaciones institucionales con la Agencia Española de Protección de Datos, sin perjuicio de la colaboración de Asesoría Jurídica, Responsable de seguridad y Responsables de las Unidades internas responsables de cada fichero.

Como consecuencia del ejercicio de las potestades que la Ley reconoce a la Directora de la Agencia Española de Protección de Datos en lo referente a solicitudes de información y acciones inspectoras, y con el fin de obtener una interlocución única ante la Agencia Española de Protección de Datos, el Departamento que reciba aviso de inspección o solicitud de información de la Agencia Española de Protección de Datos lo pondrá en conocimiento inmediatamente del Delegado de Protección de Datos, a través del correo electrónico dpd@ibermatica.com.

Para el supuesto de una Inspección, el Delegado de Protección de Datos comparecerá a dicho acto, sin que deba iniciarse la actuación inspectora sin su presencia.

En caso de notificación de procedimiento o solicitud de información se remitirá al Delegado de Protección de Datos escrito original recibido de la Agencia informando de la fecha de notificación, así como información sobre los extremos solicitados por esta última si obran en su Unidad. El Delegado de Protección de Datos remitirá la contestación que proceda a este Organismo.

12.2. Obligaciones del personal

Todo el personal de Ibermática tiene la obligación de conocer y cumplir la presente política, las normativas, medidas y procedimientos derivados de la misma.

El incumplimiento de la presente Política de Protección de Datos o la normativa, medidas y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

12.3. Consultas

Cualquier consulta en relación con la presente política, podrá ser dirigida a la dirección de email: dppo@ibermatica.com o rgpd@ibermatica.com



13. Controles para el adecuado cumplimiento de esta política

De manera trimestral el DPD de Ibermática S.A. verificará el registro a los efectos de ver las últimas actualizaciones y se reunirá con los responsables de tratamiento para controlar la correcta cumplimentación del mismo.

Cada seis meses el DPD se llevarán al Comité de RGPD las deficiencias detectadas, así como la propuesta de aspectos de mejora.

Una vez al año se evaluará esta política respecto de las incidencias detectadas a los efectos de incorporar las posibles mejoras.

14. Revisión

Esta política deberá ser revisada al menos una vez al año, debiendo actualizarse al efecto; al igual que la documentación que pueda formar parte o referenciada por ésta.

15. Validez y gestión documental

Esta política es válida, con efecto retroactivo, a partir de 25 de mayo de 2018.