CERTIFICACIÓN CUMPLIMIENTO NORMATIVA PROTECCIÓN DE DATOS PERSONALES DE

ASOCIACIÓN PLATAFORMA PALMERA DE ATENCIÓN INTEGRAL A LA DISCAPACIDAD

- INDISPAL -

Fecha: Julio de 2026.

El presente Documento se realiza en cumplimiento de las exigencias establecidas por 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 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

El RGPD, establece en el artículo 5 los principios relativos al tratamiento de datos personales:

- Licitud, lealtad y transparencia: Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.
- Limitación de la finalidad: Los datos se deben recoger con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- Minimización de datos: Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Exactitud: Los datos deben ser exactos, y si fuera necesario, actualizados. Además, se establece que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación si los datos son inexactos con respecto a los finales para los que se tratan.
- Limitación del plazo de conservación: Los datos deben ser 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.
- Integridad y confidencialidad: Los datos deben ser tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas de control apropiadas.

1. DATOS GENERALES

- **RESPONSABLE DEL TRATAMIENTO**

ASOCIACIÓN PLATAFORMA PALMERA DE ATENCIÓN INTEGRAL A LA DISCAPACIDAD (INDISPAL).
CIF: G-38695961.
Dirección: Calle Félix Duarte Pérez, Número 14, Local 1, 38712, Breña Baja, La Palma, Santa Cruz de Tenerife, España.
Teléfono: +34 922.181.213.
Correo electrónico: indispal@indispal.es.
Número de Registro de Asociaciones de Canarias: G1/S1/12998-02/P.
Número de Registro de Entidades Colaboradoras en la prestación de Servicios Sociales: SC/LP/03/760.

- **DELEGADO DE PROTECCIÓN DE DATOS (DPD)**

En cumplimiento del RGPD y de la LOPDGDD, INDISPAL ha procedido a la designación de un Delegado de Protección de Datos, notificándolo ante la Autoridad de Control, siendo en el caso de España, la Agencia Española de Protección de Datos (AEPD). Se adjunta notificación a la AEPD.

AFONSO & GONZÁLEZ ASESORES, S.L., DPD-ES2111220. Certificado por el Centro de Registro y Certificación de Personas (CERPER) de Conformidad con el Esquema de Certificación de DPD de la AEPD.
Correo electrónico: dpd@aygasesores.net.

2. SOBRE EL REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO (RAT)

La definición de las actividades de tratamiento es un paso fundamental que requiere tener claro las finalidades del tratamiento de datos personales.

El artículo 30, apartado 1 del RGPD obliga a los Responsables del Tratamiento a llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. La identificación y descripción de las actividades de tratamiento, no sólo es una obligación, sino una necesidad para facilitar el análisis de riesgos.

Relacionamos a continuación las Actividades de Tratamiento llevadas a cabo.

Nº	NOMBRE	FORMA DE TRATAMIENTO
1	GESTIÓN DE SOCIOS	MIXTO
2	GESTIÓN DE RECURSOS HUMANOS	MIXTO
3	GESTIÓN DE CURRICULUM VITAE	MIXTO
4	GESTIÓN DE EMPRESAS COLABORADORAS / SOCIO COLABORADOR	MIXTO
5	GESTIÓN DE LA JUNTA DIRECTIVA	MIXTO
6	GESTIÓN DE LOS DATOS DE CONTACTO DE PERSONAS FÍSICAS DENTRO DE UNA ORGANIZACIÓN	MIXTO
7	GESTIÓN DE PROYECTOS	MIXTO

8	GESTIÓN DE LAS VIDEOCONFERENCIAS	MIXTO
9	GESTIÓN ECONÓMICA Y CONTABLE	MIXTO
10	PREVENCIÓN DEL BLANQUEO DE CAPITALES	MIXTO
11	GESTIÓN DEL PORTAL DE TRANSPARENCIA	MIXTO
12	GESTIÓN DEL CANAL DEL SISTEMA INTERNO DE INFORMACIÓN / DENUNCIAS	MIXTO
13	GESTIÓN DE LA PÁGINA WEB	MIXTO
14	GESTIÓN DE REDES SOCIALES	MIXTO
15	GESTIÓN DE LA MENSAJERÍA INSTANTÁNEA (WHATSAPP BUSINESS)	MIXTO
16	GESTIÓN DE ARCHIVO	MIXTO
17	GESTIÓN DESTRUCCIÓN DOCUMENTAL	MIXTO
18	GESTIÓN DE LAS VIOLACIONES DE LA SEGURIDAD DE LOS DATOS PERSONALES	MIXTO
19	GESTIÓN PARA LA ATENCIÓN DE LOS EJERCICIOS DE LOS DERECHOS DE LOS INTERESADOS	MIXTO

3. CUMPLIMIENTO DE LAS OBLIGACIONES POR EL RESPONSABLE DEL TRATAMIENTO

El Responsable del Tratamiento cumple con lo estipulado en la normativa de protección de datos en cuanto a:

1. Obtener el consentimiento informado, inequívoco, expreso y explícito del titular del dato personal.
2. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto del encargo. En ningún caso utiliza los datos para fines propios.
3. Facilitar al interesado titular del dato personal:
    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. Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
    e. La intención 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, 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.
    f. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
    g. La existencia del ejercicio de los derechos en materia de protección de datos previstos en los artículos del 15 al 22 del RGPD.

4. Implementar las Medidas de Seguridad que se relacionan a continuación.

Al evaluar la adecuación de las medidas establecidas INDISPAL siempre tiene en cuenta los riesgos a los que están sometidos los datos personales y su tratamiento, tanto antes de empezar éste como en el momento mismo del tratamiento, observando los posibles riesgos para la protección de los datos de los interesados, valorando la probabilidad de que sucedan, así como el impacto o daño que causarían en caso de que se materializaran, teniendo en cuenta que los riesgos a los que puede estar sometido el tratamiento de los datos puede conllevar la destrucción o pérdida de datos, la alteración accidental o ilícita o un acceso o comunicación no autorizada a dichos datos.

Una vez evaluado el riesgo existente, las medidas que INDISPAL tiene instauradas en correspondencia con el RGPD y la LOPDGDD y que son objeto de revisión y actualización de manera periódica, entre otras, son:

- Cumplimiento con el principio de protección de datos: Licitud, lealtad y transparencia.

  - Se informa al titular de los datos o su representante legal, de manera previa al inicio del tratamiento, de la identidad y los datos de contacto del responsable del tratamiento, de los datos de contacto del delegado de protección de datos, si procediere, de los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento, así como del resto de información establecida en el artículo 13 del RGPD, aportándola de forma concisa, transparente, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo, a través de cuestionarios, formularios, modelos con políticas de protección de datos que reflejan las cláusulas de privacidad.

  - Cuando la base de legitimación del tratamiento es el consentimiento del interesado se han articulado procedimientos para permitirles su revocación en cualquier momento.

  - Se ha instaurado un procedimiento que permite a los interesados actualizar o modificar los datos proporcionados.

- Cumplimiento de los principios de protección de datos: Minimización de datos y Limitación de la finalidad.

  - Se recaban solo los datos personales necesarios en función de la finalidad, con fines determinados, explícitos y legítimos para evitar tratar datos innecesarios.

  - Se recaban solo datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

  - La LOPDGDD, recoge en su Artículo 32. Bloqueo de los datos: 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 las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

  - Transcurrido el plazo de prescripción de las acciones, INDISPAL procede a la destrucción/ borrado/supresión de los datos personales con medidas de seguridad adecuadas para garantizar la destrucción total de los mismos.

- Cumplimiento del principio de protección de datos: Exactitud.

  Los datos personales se mantienen actualizados, adoptando todas las medidas para rectificarlos o suprimirlos sin dilación en el caso que sean inexactos con respecto a los fines para los que se tratan.

- Cumplimiento del principio de protección de datos: Limitación del plazo de conservación.

  Los datos personales son mantenidos de forma que se permite la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.

- Cumplimiento del principio de protección de datos de: Integridad y confidencialidad.

  Ha tenido en cuenta el análisis de riesgos efectuado y el establecimiento de respuestas a las amenazas que afectan a los objetivos de seguridad relacionados con la privacidad:

  - Ha instaurado medidas para impedir accesos no autorizados a los sistemas: Principio de Confidencialidad. Garantiza la confidencialidad de la información por la cual ésta no es vista o accedida por personas no autorizadas.

  - Ha instaurado medidas para evitar modificaciones no autorizadas de la información: Principio de Integridad. Garantiza la integridad desde el prisma de que la información es veraz y corresponde a la situación real de la persona y no es manipulada por nadie no autorizado.

  - Ha instaurado medidas para asegurar que sea posible acceder a los datos sólo cuando sea necesario: Principio de Disponibilidad. Garantiza la disponibilidad desde la óptica de que la información está accesible cuando se necesita.

- Medidas organizativas

  - Los trabajadores con acceso a los datos personales están agrupados por perfiles, detallando los datos y recursos a los que cada perfil ha de tener acceso.

  - Ha establecido protocolos para conceder las autorizaciones de acceso o revocarlas cuando el trabajador ya no esté en la Entidad.

  - Suscribe con los trabajadores los compromisos de confidencialidad y deber de secreto sobre los datos personales a los que acceden.

  - Revisa las políticas internas que delimitan claramente las responsabilidades de los trabajadores.

  - Imparte formaciones en materia de protección de datos personales a la plantilla.

  - Trata por sí mismo los datos y, en su caso, a través de terceros debidamente autorizados por los interesados o con los que mantiene contratos de Encargado del Tratamiento adaptados a la normativa vigente.

- Medidas técnicas

  - Establecimiento de ID de usuario y contraseñas para acceder a la información.

  - Establecimiento de un control y registro de accesos a los datos para que solo accedan los usuarios autorizados.

  - Control de acceso físico a los lugares donde se almacenan los datos.

- Gestión de altas y bajas en el registro de trabajadores con acceso a los datos.
- Gestión de los perfiles de acceso.
- Gestión de perfiles de acceso con privilegios especiales.
- Gestión de la información confidencial de autenticación.
- Contraseñas diferentes, cambiadas de forma periódica.
- Revisión de los perfiles de acceso, así como la revocación o modificación de dichos perfiles de acceso.
- Control de accesos a redes y servicios asociados.
- Se han instaurado restricciones de acceso a la información.
- Se han establecido procedimientos de limitación de accesos por puestos de trabajo.
- Existen procedimientos seguros de inicio de sesión.
- Ha implementado un sistema de gestión de contraseñas para la autenticación.

➢ Seguridad física

- Áreas seguras.
  - Se ha instaurado el perímetro de seguridad física.
  - Controles físicos de entrada.
  - Seguridad de oficinas, despacho y recursos.
  - Política de mesas limpias.
  - Uso mínimo de papel o de soportes similares.
  - Destructora de documentos.
  - Armarios propios con cerraduras específicas.
  - Documentos clasificados y etiquetados.
  - Lugares de trabajo protegidos con medidas de seguridad, con imposibilidad de acceso a personas no autorizadas.

- Seguridad de los equipos. Para garantizar la seguridad de los equipos, se ha considerado:
  - Emplazamiento y protección de los equipos.
  - Las instalaciones de suministro, la seguridad del cableado, el mantenimiento de equipos.
  - La salida de activos fuera de las dependencias de la Entidad.
  - La seguridad de equipos y activos fuera de las instalaciones.
  - La reutilización o retirada segura de dispositivos de almacenamiento.
  - Bloqueo de pantalla cuando el equipo informático esté desatendido por el usuario.

➢ Seguridad de las operaciones

- Para salvaguardar la seguridad de la información en las operaciones, se han establecido controles respecto a las responsabilidades y los procedimientos de las operaciones:
- Protección y Controles contra malware.

- Copias de seguridad. Realiza periódicamente copias de seguridad.
- Registro de actividad y supervisión.
- Control del software en explotación. Utiliza sólo software original, actualizado y con licencia oficial.
- Gestión de las vulnerabilidades técnicas y de las consideraciones de las auditorías de los sistemas de información.
- Restricciones en la instalación de software.
- Firewall y sistemas actualizados de protección en todos los terminales.

➢ Seguridad de las comunicaciones

- Para proteger la información que se comunica por redes telemáticas y sus infraestructuras se han establecido:
  - Controles para gestionar la seguridad en las redes y para las transferencias de información a través de los controles de red.
  - Mecanismos de seguridad asociados a servicios en red, así como la segregación de redes.
  - Políticas y procedimientos de intercambio de información: Acuerdos de confidencialidad y no divulgación suscritos; La seguridad de las comunicaciones en servicios de aplicación accesibles por redes públicas; Políticas de desarrollo seguro de software; Procedimientos de control de cambios en los sistemas; Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo; Restricciones a los cambios en los paquetes de software.

➢ Seudonimiza la información tratada.

Aplica la seudonimización o el tratamiento de datos personales de manera que no pueden atribuirse a un interesado dichos datos sin utilizar información adicional. Utiliza códigos que sustituyen los datos identificativos de un interesado, este código y los datos identificativos figuran por separado, en archivos encriptados que hacen que no pueda atribuirse directamente la identificación del titular si no se tiene el código que lo ha sustituido, además de la clave de desencriptado. Esta medida permite generar más seguridad en el tratamiento porque, aunque se sustrajera esa información, al no disponerse ni de la clave, ni de la relación de códigos e interesados no podrán atribuir esa información a un sujeto en concreto.

➢ Cifra la información.

- Cifra la información transmitida por redes públicas de telecomunicaciones, así como el acceso a los dispositivos extraíbles que utilizan, de tal forma que, si se accede a un correo electrónico con documentos adjuntos o si se extravía un dispositivo que contenga datos personales, la opción instaurada de cifrado hace que sea inteligible y que, no pueda accederse a los datos que contiene el correo electrónico o el dispositivo.

- Ha implementado políticas sobre el uso de controles de cifrado, así como, sobre la gestión de claves.

➢ Gestión de incidentes de seguridad de la información

- Establecimiento de responsabilidades y procedimientos para la notificación de las incidencias y violaciones de seguridad.

- Valoración y adopción de decisiones ante posibles eventos de seguridad de la información.
- Procedimiento de respuesta a los incidentes de seguridad.
- Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- Procedimiento de gestión de la notificación a la Autoridad de Control y a los interesados, si procediere.

➢ Realización de controles periódicos, con el fin de evaluar, valorar, verificar la eficacia y efectividad real de las medidas técnicas y organizativas implantadas para garantizar el nivel de seguridad.

➢ Criterios de utilización de dispositivos digitales

El correo electrónico y los demás dispositivos de almacenamiento de datos o de comunicación, así como los terminales fijos o móviles son herramientas exclusivamente de trabajo para el desempeño de las funciones laborales según contrato laboral, no pudiendo ser utilizadas para fines personales, domésticos o para fines profesionales diferentes a los convenidos. INDISPAL informa a los trabajadores sobre dichos usos, así como sobre el acceso al contenido derivado del uso de estos medios a los solos efectos de verificar el cumplimiento de las obligaciones laborales, estatutarias establecidas para garantizar la integridad de dichos dispositivos. En todo caso, los accesos se harán conforme a la normativa de protección de datos y velando por la protección de la intimidad de los afectados.

Los trabajadores no podrán permitir el acceso de terceros a las cuentas y los dispositivos que les hubieran sido confiados por INDISPAL por motivo de su relación laboral. Una vez cesado el motivo del que trajese causa la entrega, se retiran las credenciales al trabajador y se suprime el contenido, siendo bloqueados por el tiempo oportuno.

➢ Procedimiento para el Ejercicio de los Derechos de los Interesados.

- Existe instaurado un procedimiento para la recepción y respuesta de los ejercicios de los derechos de los interesados conocido por todos los trabajadores y por los responsables según la función que realizan dentro de la Entidad.
- Existen modelos que se le facilitarían a los interesados, si así lo solicitaren, para el ejercicio de sus derechos.
- Se informa a los interesados, a través de las cláusulas de protección de datos consignadas en todos los formularios donde se recaban datos personales, de la posibilidad de ejercitar los derechos y la forma en que puede realizarlo.
- Se ha revisado y actualizado el procedimiento existente.

➢ Protocolo de supresión de datos y destrucción de soportes.

Se suprimen los datos en local, así como las copias de respaldo de éstos en servidores de almacenamiento y en soportes de respaldo ubicados en lugares diferentes al de trabajo habitual.

Se exceptúan los casos en los que se solicita la supresión cuando existe justificación legal, que se documenta en cada caso, para mantener o custodiar el dato más allá de la prestación del servicio.

La destrucción de soportes se realiza garantizando físicamente la imposibilidad de extraer los datos.

4. DE LAS MEDIDAS DE SEGURIDAD

MEDIDA	DESCRIPCIÓN
Debida diligencia con los Encargados del Tratamiento.	Se identifica adecuadamente a los Encargados del Tratamiento con accesos a datos personales, suscribiendo el contrato de encargado del tratamiento conforme al artículo 28 del RGPD.
Debida diligencia con los Prestadores de servicios sin acceso a datos personales.	Se adoptan las medidas adecuadas para impedir el acceso a datos personales en aquellos supuestos en que no es necesario para la prestación de los servicios.
Delegación de autorizaciones.	Establecimiento de perfiles de usuarios (personal autorizado); Llevanza de un control de acceso; Definidas las funciones y obligaciones del personal, según categorías; Identificación y Autenticación diferenciada del personal.
Acceso a datos a través de redes de comunicaciones.	Configurado el acceso a datos personales a través de redes de comunicaciones de modo que garantice las mismas medidas de seguridad que en modo local y es acorde a los niveles de seguridad aplicables a los datos accedidos.
Régimen de trabajo fuera de los locales.	Establecimiento de un procedimiento interno para la solicitud de tratamiento de datos fuera de los locales. Para obtener este tipo de acceso el trabajador deberá solicitar autorización al Responsable de Privacidad, quedando justificación documental de la autorización. No se prevé tratamiento de datos fuera de los locales titularidad del Responsable del Tratamiento.
Ficheros temporales o copias de trabajo de documentos.	Establecimiento de una política adecuada para la generación, uso y destrucción dando cumplimiento a los niveles de seguridad que le resulten de aplicación.
Funciones y obligaciones del personal.	Definidas las medidas necesarias en materia de seguridad que el personal necesita conocer. Formación continuada al personal.
Registro de incidencias.	Establecimiento de un procedimiento de notificación, gestión y registro de incidencias de seguridad de los datos.
Control de acceso.	Se ha establecido el acceso del personal únicamente a recursos que precisa. El personal autorizado para acceder a la información y la relación de los mismos se regula a través de servicios de directorio de red y en las distintas aplicaciones. Exclusivamente el personal designado podrá conceder, alterar o anular los accesos autorizados conforme a los criterios establecidos.
Controles periódicos de verificación de cumplimiento.	Realización de controles periódicos de verificación de la eficacia de las medidas adoptadas para el cumplimiento legal.
Auditoría.	Se realizan auditorías de la eficacia de las medidas de seguridad técnicas y organizativas adoptadas con la periodicidad establecida.
Identificación y autenticación.	Se garantiza la correcta identificación y autenticación del personal autorizado de forma inequívoca y personalizada. Existe un procedimiento de asignación, distribución, almacenamiento y cambio de contraseñas que garantiza su confidencialidad e integridad y su modificación con una

	periodicidad adecuada. Las contraseñas se almacenan de forma ininteligible.
Copias de respaldo y recuperación.	Se ha establecido un sistema adecuado de realización de copias de respaldo y ejecución de procedimientos de recuperación. Las copias se efectúan y verifican dentro de los plazos reglamentariamente estipulados. Se conserva una copia de respaldo cifrada en un lugar diferente de aquel en que se encuentren los equipos informáticos que contienen el sistema de información.
Criterios de archivo.	Se ha establecido criterios de archivo de los documentos que contienen datos personales, de modo que se garantice la correcta conservación de los documentos, la localización y consulta de la información y se posibilita el ejercicio de los derechos de acceso, rectificación y supresión de los datos, así como otros derechos, como se regula en la normativa de protección de datos.
Dispositivos de Almacenamiento.	Establecimiento y verificación que todos los documentos que contienen información personal se almacenan en dispositivos que cuentan con medios para impedir el acceso a personal no autorizado.
Custodia de Documentos.	Se han definido políticas que permiten acreditar que el personal ha sido informado de sus obligaciones de custodia respecto de aquella documentación que no se encuentra debidamente almacenada por estar en proceso de revisión o tramitación.
Seudonimización.	Aplicación de procedimientos de segregación de información que impidan atribuir los datos a una persona identificable.
Procedimiento de recuperación y resiliencia.	Establecimiento de mecanismos para la recuperación de los servicios y sistemas que gestionen datos personales.
Restauración de acceso a los datos.	Establecimiento de procedimientos de restauración de la disponibilidad y el acceso en caso de incidente físico o técnico.
Confidencialidad de los datos.	Establecimiento de políticas que recogen el deber de confidencialidad y secreto del personal con acceso a los datos.
Integridad de los datos.	Establecimiento de mecanismos para evitar la manipulación y modificación de datos.
Gestión de soportes.	Establecimiento de un procedimiento que garantice no se almacenen datos especialmente protegidos en soportes distintos de los discos de copia de seguridad. La identificación de los soportes estará codificada. La distribución de los soportes se realizará cifrando dichos datos o bien utilizando otros mecanismos que garanticen su confidencialidad e integridad. Asimismo, se cifran los datos contenidos en dispositivos portátiles.

5. DEBER DE CONFIDENCIALIDAD

INDISPAL se compromete a guardar la máxima reserva y secreto sobre la información clasificada como confidencial. Se considerará información confidencial cualquier dato al que pudiere accederse en virtud de la prestación de servicios suscrita y en especial la información y datos a los que haya accedido o acceda durante la ejecución de ésta.

El deber de secreto y confidencialidad que se deriva de la prestación de servicios obliga a INDISPAL durante su vigencia y se extenderá, en función de la tipología de información objeto del tratamiento, durante los plazos máximos previstos en la legislación vigente que resulte de aplicación. La obligación de confidencialidad tendrá carácter indefinido, manteniéndose permanentemente en vigor con posterioridad a la finalización, por cualquier causa, de la relación entre las partes.

INDISPAL garantiza que las personas autorizadas para tratar datos personales se comprometen, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes. Por personas autorizadas debe entenderse toda persona que, con independencia de la naturaleza jurídica del vínculo que le une a INDISPAL, por cualquier medio, puedan tener acceso a los datos objeto de tratamiento.

6. GESTIÓN DE LAS VIOLACIONES DE LA SEGURIDAD DE LOS DATOS PERSONALES

Se ha establecido un procedimiento para la gestión y notificación de las violaciones de la seguridad, tanto a la Autoridad de Control, como a los interesados si así procediere, así como de controles periódicos de verificación de cumplimiento de dichos procedimientos. Llevanza del procedimiento a través de AFONSO & GONZÁLEZ ASESORES, S.L.

7. GESTIÓN DE LOS EJERCICIOS DE LOS DERECHOS DE LOS INTERESADOS.

Cualquier persona o interesado tiene derecho a obtener confirmación sobre si el Responsable del Tratamiento trata datos personales que le conciernan o no. Podrá solicitar el ejercicio de los siguientes derechos presentando un escrito ante el Responsable del Tratamiento a través de sus datos de contacto:

1. Derecho de acceso: permite al interesado conocer y obtener información sobre sus datos personales sometidos a tratamiento.
2. Derecho de rectificación: permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto del tratamiento.
3. Derecho de supresión: permite que se supriman los datos que resulten ser inadecuados o excesivos.
4. Derecho de oposición: derecho del interesado a que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, en cuyo caso, únicamente se conservarán por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.
5. Derecho a la limitación del tratamiento: conlleva el marcado de los datos personales conservados, con la finalidad de limitar su futuro tratamiento, en cuyo caso, únicamente se conservarán para el ejercicio o la defensa de reclamaciones.
6. Derecho a la portabilidad de los datos: facilitar al interesado los datos objeto de tratamiento, a fin de que éste pueda transmitirlos a otro responsable, sin impedimentos. Como interesado, tiene derecho a recibir los datos personales que le incumban, que haya facilitado y en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento cuando: El tratamiento esté basado en el consentimiento, los datos hayan sido facilitados por la persona interesada y el tratamiento se efectúe por medios automatizados. Al ejercer su derecho a la portabilidad de los datos, tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
7. Derecho a no ser objeto de decisiones individuales automatizadas (incluida la elaboración de perfiles): derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos o afecte significativamente de modo similar.

El interesado podrá retirar su consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento previo a su retirada, así como presentar una reclamación ante la Autoridad de Control, siendo en el caso de España, la Agencia Española de Protección de Datos (AEPD), cuando no haya obtenido satisfacción en el ejercicio de sus derechos o considere que hemos tratado sus datos de manera inadecuada. Para contactar con la AEPD puede hacerlo a través de su página web https://www.aepd.es/ o de la dirección postal Paseo de la Castellana, Número 141, Edificio Cuzco IV, 28046, Madrid, España.

Se ha establecido un procedimiento para la gestión y tramitación de los ejercicios de los derechos de los interesados, así como controles periódicos de verificación de cumplimiento de dichos procedimientos. Llevanza del procedimiento a través de AFONSO & GONZÁLEZ ASESORES, S.L.

8. EXPEDIENTES ABIERTOS ANTE LA AUTORIDAD DE CONTROL

A fecha del presente nunca han sido incoados expedientes ante la Autoridad de Control, siendo en el caso de España, la Agencia Española de Protección de Datos (AEPD).

9. CUMPLIMIENTO DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

En todo momento se mantiene actualizado el sistema de tratamiento, soportes informáticos, así como el contenido de la información tratada, revisando los cambios que pudieren repercutir en el cumplimiento de las medidas de seguridad implantadas, adecuándose a las disposiciones vigentes en materia de seguridad de los datos personales, así como en la normativa vigente de aplicación.

El Responsable del Tratamiento cumple con las obligaciones establecidas en 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 (RGPD), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y en la Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE), así como con lo dispuesto en otras normativas sectoriales de aplicación.

En Santa Cruz de Tenerife, a los 14 días del mes de julio de 2026.

Fdo.: AFONSO & GONZALEZ ASESORES, S.L.
Firmado digitalmente por 42265351E AYMEE GONZALEZ (R: B38820007)
Fecha: 2026.07.14 16:46:34 +01'00'

ANEXO I. NOTIFICACIÓN DESIGNACIÓN DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

Registro General de Protección de Datos

AYMEE GONZALEZ ROSELLO
MADRESELVA, NUM 3
38360 - URBANIZACION LOS NARANJOS, EL SAUZAL

SANTA CRUZ DE TENERIFE

Tipo de operación: Alta

Nº Registro Salida: 078986/2019

En relación con la notificación recibida en esta Agencia con registro de entrada 040500/2019 se ha procedido a incluir en la lista prevista en el artículo 34.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales la información correspondiente al Delegado de Protección de Datos AFONSO & GONZALEZ ASESORES, S.L. - B38820007 (Persona de contacto: AYMEE GONZALEZ ROSELLO) de la entidad o entidades que se relacionan a continuación.

NIF	ENTIDAD
G38695961	ASOCIACION PLATAFORMA PALMERA DE ATENCION INTEGRAL A LA DISCAPACIDAD (INDISPAL)

C/ Jorge Juan, 6
28001 - Madrid

T + 34 901 100 099

www.aepd.es

Código Seguro De Verificación:	APDPFE9E810A9F13DAA2C4C80-61737	Fecha	31/10/2019
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.		
Firmado Por	Subdirección General del Registro General de Protección de Datos Juan Carlos Martin Prieto		
Url De Verificación	https://sedeagpd.gob.es	Página	1/1