POLÍTICA GENERAL DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

ORPEA Ibérica

Versión : 2.0
Fecha : Mayo 2019

INTRODUCCIÓN

En ORPEA Ibérica S.A.U y sus sociedades filiales (en adelante, "Grupo ORPEA Ibérica" o simplemente "ORPEA") estamos comprometidos a desarrollar nuestra actividad con el máximo respeto a la intimidad de nuestros empleados y pacientes. Este compromiso se refleja en nuestro Código de Conducta, cuyo segundo principio establece que *"el Grupo ORPEA se compromete a respetar estrictamente los datos de carácter personal y la legislación vigente en materia de protección de datos"*.

En este sentido, desde la entrada en vigor del Reglamento General de Protección de Datos (RGPD) se han establecido una serie de obligaciones que debemos cumplir para adaptarnos a lo que el nuevo marco nos exige.

Una de las principales novedades que incluye el Reglamento es el principio de responsabilidad proactiva (*accountability*). Dicho principio impone que apliquemos medidas de seguridad técnicas y organizativas para que garantizar el cumplimiento de las normas y proteger los datos personales.

Por eso, todos los que formamos parte de ORPEA debemos fomentar activamente la cultura de la protección de datos, asegurándonos de que todos conocemos nuestros derechos y obligaciones.

La finalidad de esta Política es establecer los objetivos de gestión de la privacidad, orientando e informando sobre distintos aspectos que debemos saber sobre la protección de los datos de carácter personal en ORPEA.

ÁMBITO DE APLICACIÓN

Las reglas y pautas que se contienen y desarrollan en la presente política son de aplicación a todo el personal, los equipos y los sistemas relacionados con tratamientos, usos o medios del Grupo ORPEA Ibérica que contengan datos de carácter personal.

Quedan especialmente vinculados a esa Política:

a. todos aquellos empleados o personas que actúen en nombre y representación de ORPEA que estén involucrados en cualquier operación o conjunto de operaciones realizada sobre datos personales so conjuntos de datos personales, ya sea por procedimientos automatizados o no, que impliquen 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 de datos personales.

b. todos los recursos de los sistemas de información por medio de los cuales se puede acceder a los ficheros, tratamientos o usos que contienen datos de carácter personal, así como todos los dispositivos que efectúen cualquier proceso de tratamiento o almacenamiento de datos de carácter personal.

Cualquier violación de esta política podría exponer a ORPEA, a sus empleados y/o terceros que actúe en su nombre a importantes sanciones administrativas, penales y/o disciplinarias.

DEFINICIONES

Dato personal:	Un dato personal es cualquier información que identifique, o haga identificable a una persona física.
Dato de salud:	Los datos de salud o "datos sanitarios", son todos aquellos datos relativos al estado de salud física o mental, presente, pasada o futura, de una persona física. Algunos ejemplos son: 1) datos de enfermedad. 2) datos de discapacidad. 3) el historial clínico. 4) cualquier informe médico. 5) los tratamientos médicos. 6) el estado fisiológico o biomédico de la persona. 7) el riesgo de padecer enfermedades. 8) cualquier número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios.
Afectado/ interesado	Es la persona física titular de los datos que son objeto de tratamiento.
Tratamiento:	Un tratamiento es cualquier operación o conjunto de operaciones realizadas sobre los datos personales, por ejemplo: 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. Por nuestra propia actividad, ORPEA trata "*datos personales de salud*", que conforme a la regulación vigente están especialmente protegidos.

Historia clínica	Es el documento o conjunto de documentos que contienen toda la información de utilidad clínica relativa a un residente en el centro. La finalidad principal de la Historia Clínica es posibilitar y facilitar la asistencia sanitaria al residente, recogiendo en ella toda la información clínica necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y actualizado de su estado de salud por los sanitarios que le atienden así como el seguimiento del proceso asistencial. **La gestión y protección de los datos de salud contenidos en los historiales clínicos de pacientes y residentes es objeto de regulación en un documento interno distinto a esta Política.**

PRINCIPIOS DE TRATAMIENTO EN ORPEA

En ORPEA seguimos una política de **transparencia, lealtad y licitud de los datos:**

a. **Licitud**: Sólo trataremos los datos personales para fines específicos, explícitos y legítimos, amparados en alguna de las bases jurídicas permitidas por la legislación y sin poder ser tratados posteriormente de manera incompatible con dichos fines.

b. **Transparencia**: Solo procesaremos los datos personales en la manera que se haya informado a los interesados. Esta información deberá abarcar la finalidad del tratamiento, su base legal y la posibilidad de ejercer sus derechos.

c. **Minimización de datos y proporcionalidad**: Nos aseguraremos de que solo tratamos los datos personales que sea necesarios, adecuados, pertinentes y no excesivos para el propósito del tratamiento.

d. **Exactitud**: los datos de carácter personal debe ser exactos y mantenerse completos y actualizados de tal manera que permitan el cumplimiento de las finalidades para las que fueron recabados.

e. **Retención y eliminación**: Conservaremos los datos personales solo durante el tiempo que sea necesario en relación con los fines del tratamiento. Los datos personales que ya no sean necesarios transcurrido los plazos legales o establecidos para el tratamiento, serán eliminados.

f. **Confidencialidad y seguridad de datos**: Estamos obligados a aplicar las normas establecidas para proteger los datos personales que procesamos, tanto desde la perspectiva de la seguridad técnica como de la seguridad de la organización. A este respecto, se aplica el principio de "necesidad de saber", de modo que sólo podemos acceder la información personal que sea necesaria para el correcto desempeño de nuestras funciones, estando prohibido usar datos personales con fines privados o comerciales, para divulgarlos o ponerlos a disposición de terceros de cualquier otra forma. Esta obligación permanecerá en vigor incluso después de que nuestra relación profesional haya terminado.

REGLAS RELATIVAS A LOS TRATAMIENTOS

El Grupo ORPEA Ibérica, en cumplimiento de lo establecido en el art. 30 del RGPD, mantiene un Registro de Actividades de Tratamiento en el que se reflejan los tratamientos realizados, los sujetos afectados por los mismos y las medidas de seguridad técnicas y organizativas adaptadas para proteger dichos tratamientos.

Como regla general, los datos de carácter personal solo serán tratados cuando concurra alguno de los siguientes supuestos:

1. Se hayan obtenido el consentimiento libre, explicito, inequívoco e informado del interesado,
2. Cuando un interés legitimo de ORPEA justifique el tratamiento, siempre y cuando no prevalezcan los intereses legítimos, derechos o libertades de los interesados
3. Cuando el tratamiento sea preciso para el mantenimiento o el cumplimiento de una relación jurídica entre ORPEA y el interesado
4. Cunado el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre ORPEA por la legislación aplicable o sea llevada a cabo por una Administración Publica que así lo precise para el legitimo ejercicio de sus competencias
5. Cuando concurran situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del interesado o de la persona.

TRATAMIENTO DE DATOS PERSONALES DE EMPLEADOS:

Cada uno de los centros que forman parte del Grupo ORPEA Ibérica informa a sus empleados de todos los extremos legalmente exigidos, incluyendo: (i) que la recogida de los datos personales tiene como finalidad el cumplimiento de la relación contractual y el cumplimiento de las obligaciones legales impuestas a la empresa; (ii) que el tratamiento esta legitimado por la ejecución del contrato; (iii) que sus datos personales podrán ser comunicados a empresas del Grupo y entidades necesarias para el cumplimiento de las finalidades previstas.

TRATAMIENTO DE DATOS PERSONALES DE PACIENTES Y RESIDENTES:

Cada uno de los centros que forman parte del Grupo ORPEA Ibérica informa a sus pacientes y residentes de todos los extremos legalmente exigidos, incluyendo: (i) que la recogida de los datos personales tiene como finalidad el cumplimiento de la relación contractual y la prestación de los servicios de estancia y tratamiento sanitario así como realizar los servicios administrativos conexos a dichos servicios como la facturación, gestión y cobros; (ii) que el tratamiento esta legitimado por la ejecución del contrato y las obligaciones legales impuestas a las empresas del Grupo; (iii) que sus datos personales podrán ser comunicados a empresas del Grupo y centros sanitarios y/o profesionales de salud que requieran la información para cumplir con el contrato y con la obligación o requerimientos públicos o privados.

TRATAMIENTO DE DATOS PERSONALES DE CANDIDATOS:

Si un candidato manifiesta interés por trabajar en ORPEA, debe presentar su candidatura a través de la plataforma en nuestra pagina web. Esta herramienta digital garantiza el cumplimiento de la normativa de protección de datos en los procesos de selección. Solamente de forma excepcional a la vista de las circunstancias del candidato podremos aceptar su C.V. en papel tras la firma del documento *"INFORMACIÓN SOBRE PROTECCIÓN DE DATOS DE CANDIDATOS"* en el que se contienen todos los extremos relativos a la finalidad, destino y plazo de conservación de sus datos curriculares.

VIDEOVIGILANCIA:

ORPEA informa de que en sus centros e instalaciones existe de un sistema de vigilancia mediante cámaras para garantizar la seguridad de los trabajadores, residentes, pacientes, visitas y todas aquellas personas que concurran al interior del mismo, así como para poder ejercer de la función de control de la empresa, de conformidad con el art. 89 de la LOPDyGDD y el art. 20.3 del Estatuto de los Trabajadores.

La información obtenida y almacenada mediante el sistema de grabación se utilizará exclusivamente para fines de prevención, seguridad y protección de personas y bienes que se encuentren en el establecimiento o instalación sometida a protección, así como para la supervisión de la relación laboral con los empleados y depurar las responsabilidades legales y laborales que eventualmente procedan en caso de incumplimiento de los deberes y obligaciones legalmente impuestos al empleado.

LA EMPRESA garantiza que las imágenes obtenidas respetarán en todo momento los derechos fundamentales del empleado y que ningún caso supondrá un menoscabo en la honra y reputación, ni será contraria a los intereses del empleado, respetando en todo momento la Ley 1/1982, de 5 de mayo, sobre el derecho al honor, a la intimidad personal y familiar y a la propia imagen, la Ley 3/2018 sobre la Protección de Datos Personales, la demás legislación aplicable.

FOTOGRAFÍAS Y USO DE IMAGEN:

ORPEA recaba el consentimiento apropiado para el uso de las imágenes (grabación de vídeos y/o fotos) y archivos electrónicos en los que figura la imagen de pacientes, residentes, empleados y terceros con las finalidad de publicar, exponer o difundir en el centro de trabajo las fotografías y/o los videos tomados en eventos internos del propio centro, así como mostrar las distintas residencias y actividades que se realizan dentro de las mismas en la pagina web www.orpea.es, en las redes sociales y/o medios de comunicación social. En este caso, se publicarán imágenes y/o vídeos en las redes sociales en las que ORPEA tiene o pudiera tener presencia, lo que implica o pudiera implicar el acceso público a las mismas, así como la posibilidad de que sean compartidas por otras personas o páginas, sobre las que ORPEA no dispone de ningún poder de control o vinculación.

ORPEA se compromete a que el uso de este material en ningún caso supondrá un menoscabo en la honra y reputación, ni será contraria a los intereses de las personas, respetando en todo momento la Ley 1/1982, de 5 de mayo, sobre el derecho al honor, a la intimidad personal y familiar y a la propia imagen, la Ley 3/2018 sobre la Protección de Datos Personales, la demás legislación aplicable.

NAVEGACIÓN ONLINE Y COOKIES:

Las cookies son pequeños archivos de texto que se instalan en el navegador del ordenador del usuario para registrar su actividad, enviando una identificación anónima que se almacena en el mismo, con la finalidad de que la navegación sea más sencilla, permitiendo, por ejemplo, el acceso a las áreas, servicios o promociones a los usuarios que se hayan registrado previamente, evitando tener que registrarse en cada visita. Se pueden utilizar también para medir la audiencia, parámetros del tráfico y navegación, tiempo de sesión, y/o controlar el progreso y el número de entradas.

ORPEA procurará en todo momento establecer mecanismos adecuados para obtener el consentimiento del Usuario para la instalación de cookies que lo requieran.

Para más información sobre las Cookies utilizados por ORPEA y las normas de Navegación web, por favor consulte nuestra **Política de Cookies y Navegación.**

DATA PROTECTION OFFICER (DPO)

ORPEA ha nombrado a un Data Protection Officer a nivel de Grupo en cumplimiento del art. 37 del Reglamento Europeo de Protección de Datos.

Con el objetivo de garantizar que los interesados (tanto dentro como fuera de la organización) y las autoridades supervisoras puedan ponerse en contacto con el DPO de forma fácil, directa y confidencial, cumpliendo así con el Art. 37 del RGPD, ORPEA ha comunicado los datos de contacto del DPO a las autoridades supervisoras correspondientes y publica la identidad y datos de contacto del DPO:

Nombre:	Sra. Alma Benzaïd.	**Teléfono:**	+ 33 1 47 75 60 22.

Mail:	a.benzaid @orpea.net	**Dirección:**	12 rue Jean Jaurès, 92 813 Puteaux Cedex, París, Francia.

MEDIDAS DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En ORPEA hemos adoptado una serie de medida técnicas y organizativas para salvaguardar la confidencialidad y seguridad de la información que tratamos. Estas medida son:

A) Medidas de seguridad informática

El Departamento de IT ha establecido una serie de reglas para garantir la seguridad de los sistemas y medios informáticos de ORPEA que todos cumplir. Algunas de ellas son:

- Queda estrictamente prohibido el uso de memorias o discos externos (USB) sin previa autorización.
- Se exige la observancia de las licencias de software y se prohíbe el uso de software no autorizado.
- Se ejecuta software antivirus con una frecuencia definida para comprobar si los ordenadores y medios presentan alguno de los virus conocidos.
- Se revisan con regularidad el software y el contenido de datos de los sistemas y se investiga la existencia de archivos falsos o modificaciones no autorizadas.
- Se deben someter a un análisis de virus todos los medios extraíbles (discos, CD, lápices de memoria, etc.) antes de utilizarlos.
- Se debe informar de inmediato al soporte de IT de cualquier ataque de virus.
- Se deberán tratar siempre como sospechosos los datos adjuntos e hiperenlaces, de cualquier naturaleza, de un correo electrónico.
- Se debe eliminar el correo sin abrir los datos adjuntos o el enlace, siempre que llegue un correo electrónico de parte de alguien a quien no se conoce.
- Se debe llamar al remitente de un correo electrónico para confirmar el contenido de los datos adjuntos/enlaces antes de abrirlo, cuando éste nos llegue de un contacto profesional que habitualmente no envía datos adjuntos/enlaces o de quien no se esperaban datos adjunto/enlaces.

Estas y otras medidas de obligado cumplimiento se recogen en la **"POLÍTICA DE SEGURIDAD DE IT DE ORPEA IBÉRICA Y SUS FILIALES".**

B) Medidas seguridad de los datos personales en soporte de papel

- Los expedientes y carpetas deben estar archivados y organizados de forma que se garantice su correcta conservación, localización y consulta;
- Deben estar guardados en elementos o dispositivos (armarios, archivadores, etc.) con mecanismos que obstaculicen su apertura.
- Cuando no se encuentre archivada en los elementos antes mencionados, la persona que se encuentre al cargo custodiarlos e impedir en todo momento accesos no autorizados.

En ORPEA seguimos una Política de "*Clean Screen & Desks*" (Pantallas y Mesas Limpias); de forma que:

- Cada vez que abandonemos el ordenador, debemos proceder al bloqueo de la pantalla (presionando Ctr+l).
- Al acabar nuestra jornada, todos los documentos y expedientes deben estar debidamente archivados o guardados bajo llave, de forma que evitemos su perdida o sustracción.

C) Funciones del DPO

- Controlar el cumplimiento del RGPD por ORPEA.
- Asesorar a ORPEA para llevar a cabo las evaluaciones de impacto de la protección de datos.
- Considerar debidamente el riesgo asociado a las actividades de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.
- Mantener el registro de las operaciones de tratamiento, responsabilidad de ORPEA con el fin de llevar a cabo las funciones de control del cumplimiento, información y asesoramiento.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

D) Funciones y obligaciones del personal

- Todo el personal autorizado para acceder a los sistemas de información o ficheros que contengan datos de carácter personal, está obligado a cumplir la normativa de seguridad recogida en esta Política y cualquier otra que ORPEA pudiera dictar.

DERECHOS RELATIVOS A LOS DATOS PERSONALES

Los empleados, residentes, pacientes y todas las demás personas cuyos datos personales son tratados por ORPEA pueden ejercer sus derechos de acceso, rectificación, oposición, supresión, limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

Derecho de acceso: El interesado tiene derecho a solicitar y obtener gratuitamente información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. Se debe informar de:

a. La finalidad del tratamiento de sus datos
b. Las categorías (básicos, bancarios, salud...etc)
c. Los destinatarios a los que se va a comunicar.
d. El plazo para conservarlos.
e. Como solicitar al responsable el ejercicio de los derechos.
f. El derecho a presentar una reclamación a la autoridad de control.
g. Cualquier información sobre el origen de los datos.
h. Transferencias internacionales.
i. Los tratamientos y decisiones automatizadas sobre sus datos.

Derecho de rectificación: El interesado tiene derecho a obtener la rectificación de los datos personales que sean inexactos sin dilación indebida.

Derecho de oposición: El interesado tiene derecho a oponerse al tratamiento de sus datos en algunos supuestos tasados.

Derecho de supresión: El interesado tiene derecho a la eliminación de los datos de carácter personal cuando concurra alguna de las circunstancias legalmente tasadas.

Igualmente, todos los interesados podrán ejercitar sus derechos a la portabilidad de datos, limitación del tratamiento o a retirar el consentimiento previamente otorgado.

Para el ejercicio de sus derechos, el interesado deberá dirigir un correo electrónico a protecciondedatos@orpea.net, indicando el derecho que quiere ejercitar e identificándose inequívocamente mediante su DNI o documento similar válido en Derecho. En todos los casos, las solicitudes formuladas se archivarán con su fecha y copia de la contestación remitida al interesado.

Si el interesado entiende que los tratamientos realizados no se ajustan a la legalidad o que su solicitud no ha sido debidamente atendida, puede presentar reclamación ante la Agencia Española de Protección de Datos (www.aepd.es) en los términos indicados por esta.

REGISTRO Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

Se entiende por incidencia todo hecho o circunstancia que, al producirse, genere, o pueda generar, cualquier tipo de riesgo o daño que afecte a la seguridad, confidencialidad o integridad de los datos personales tratados por ORPEA, como por ejemplo los hackeos, robos de información, envío indebido de datos personales a terceros, pérdida de datos personales, etc.

Debemos estar alerta a estos sucesos e informar de ellos lo antes posible. Cualquier empleado que tenga conocimiento de cualquier incidencia se responsabiliza directa y personalmente de notificarla sin demora la Departamento de IT mediante ticket en la herramienta SNOW y al Departamento de Compliance en la siguiente dirección: protecciondedatos@orpea.net.

El DPO documentará cualquier violación de seguridad de los datos, incluidos los hechos relacionados con ella, sus efectos y las medidas de seguridad implementadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el artículo 33 del RGPD.

En caso de violación de seguridad que afecte de forma grave a los derechos y libertades de los interesados, el DPO notificará a la autoridad de control competente sin dilación indebida con un máximo de 72 horas. La comunicación a los afectados debe ser clara y sencilla.

CONTROLES PERIÓDICOS Y AUDITORÍA

Para la correcta verificación del cumplimiento de las medidas, normas y procedimientos establecidos en esta Política, de tal forma que pueda detectarse cualquier anomalía que afecte a la seguridad, integridad o disponibilidad de los datos personales contenidos en los ficheros, se realizarán, controles periódicos.

El calendario de controles y las medidas a auditar serán aprobadas por el Departamento de IT y el Departamento de Compliance anualmente.

FORMACIÓN Y PUESTA EN CONOCIMIENTO

Esta política y cualesquiera otras en materia de protección de datos es accesible al personal y se entregará una copia de la misma, en los extremos que le conciernan, a todo usuario que lo solicite.

El personal debe estar sensibilizado en esta materia mediante información, comunicados interno o por formación específica.

El incumplimiento de las obligaciones en materia de protección de datos puede podrá considerarse como un quebranto de la buena fe contractual. Si el incumplimiento tuviera carácter doloso, se emprenderán las acciones legales correspondientes para la debida depuración de responsabilidades.