

# Política global de privacidad

<b>Documento</b>	<b>Política global de privacidad</b>
<b>Propósito</b>	Regular los objetivos y criterios del tratamiento de datos personales.
<b>Aprobador</b>	Comité de Riesgos y Cumplimiento (" <b>CRC</b> ")

**Confidencialidad** - La distribución de este documento está limitada a todas las entidades del Grupo Uriach y a sus socios comerciales. No debe distribuirse más sin el consentimiento del Consejo de Administración.

## 00 INTRODUCCIÓN

Los términos utilizados en la presente Política Global de Privacidad (la "**Política**") tendrán el significado establecido 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 ("**RGPD**"), salvo que se establezca expresamente otro significado en la presente Política

## 01 OBJETIVO

El objetivo de esta Política es garantizar que cada empresa de Uriach cumpla con la normativa aplicable en materia de protección de datos, es decir, el GDPR y la normativa local de cada territorio en el que Uriach opera (la "**Normativa aplicable en materia de PD**").

Esta Política se adaptará a los cambios legislativos de los países en los que Uriach opera, así como a los criterios establecidos por la autoridad de control local competente, el Comité Europeo de Protección de Datos ("**CEPD**") y las sentencias de los tribunales competentes.

## 02 ALCANCE

El ámbito de aplicación de esta Política incluye lo siguiente:

- a) **Ámbito Corporativo** - Esta Política aplica a todas las empresas pertenecientes a Uriach, así como a las filiales y empresas participadas sobre las que Uriach tenga control efectivo o desempeñe cargos en los órganos de dirección.
- b) **Personal** - Esta Política se aplica a todos los niveles de la organización, incluidos la dirección, la alta dirección, los órganos de supervisión y todo el personal.
- c) **Ámbito relacional** - El ámbito de aplicación de esta Política se extenderá, en la medida de lo posible, a proveedores, clientes, empresas subcontratadas o empleados.
- d) **Ámbito geográfico** - Esta Política se aplica a cualquier zona geográfica en la que Uriach tenga sus instalaciones, ya sea local o internacional.

Cualquier excepción a las normas establecidas en esta Política está sujeta a la aprobación explícita del Comité de Riesgos y Cumplimiento ("**CRC**"). En caso de discrepancia o duda con respecto a esta Política, el departamento legal ofrecerá la orientación y asistencia pertinentes.

## 03 ACTIVIDADES DE TRATAMIENTO DE DATOS Y RIESGOS

La actividad principal de Uriach se desarrolla en el sector *healthcare*. Las operaciones de tratamiento de datos personales más habituales en este sector son las siguientes:

1. Contratación de personal
2. Gestión del empleo
3. Relaciones con los clientes B2C
4. Relaciones con los clientes B2B
5. Relaciones con los proveedores
6. Marketing
7. Atención al cliente
8. Farmacovigilancia, cosmetovigilancia
9. Ensayos clínicos, estudios observacionales
10. Comercio electrónico
11. Finanzas
12. Legal

Los principales riesgos derivados del incumplimiento de las obligaciones legales establecidas en la normativa aplicable en materia de PD son los siguientes:

13. Sanciones administrativas
14. Intervención reglamentaria
15. Cuestiones de calidad
16. Daños y perjuicios
17. Daños a la reputación
18. Delitos contra la intimidad

La protección de los datos personales es un objetivo prioritario para Uriach y requiere una serie de medidas legales, técnicas y organizativas que se resumen en esta Política y que se recogerán en las normas, protocolos y/o procedimientos de la empresa que correspondan.

#### 04 PRINCIPIOS DE PROTECCIÓN DE DATOS

- a) **Legitimación:** Solo se tratarán los datos personales para los que Uriach tenga una base legítima establecida por la ley.
- b) **Transparencia:** Uriach informará a los interesados de forma clara y sencilla de todas las circunstancias relativas al tratamiento.
- c) **Equidad:** Uriach no tratará los datos personales en circunstancias distintas a las comunicadas.
- d) **Limitación de la finalidad:** Uriach recabará los datos personales para fines determinados, explícitos y legítimos y no los tratará posteriormente de manera incompatible con dichos fines.
- e) **Minimización de datos:** Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se traten.
- f) **Exactitud:** Los datos personales serán exactos y se mantendrán actualizados. Uriach adoptará todas las medidas razonables para garantizar que los datos personales que sean inexactos en relación con los fines para los que se tratan se supriman o se rectifiquen sin demora.
- g) **Limitación del tratamiento:** Uriach conservará los datos personales en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos.
- h) **Integridad y confidencialidad:** Uriach tratará los datos personales de forma que se garantice una seguridad adecuada, mediante la aplicación de medidas técnicas y organizativas apropiadas. Los datos personales solo serán accesibles a las personas autorizadas a acceder a ellos y no podrán comunicarse a terceros sin la autorización y la base jurídica correspondientes.
- i) **Responsabilidad:** Cada empresa de Uriach es responsable del cumplimiento de las disposiciones de su respectiva Normativa Aplicable en materia de PD y deberá ser capaz de demostrar dicho cumplimiento.

- j) **Protección de datos desde el diseño y por defecto:** En la fase de diseño de nuevos tratamientos, proyectos, servicios y productos que impliquen el tratamiento de datos personales, Uriach realizará una evaluación previa del impacto sobre la protección de datos.

## 05 ÓRGANOS DE CONTROL, FUNCIONES Y RESPONSABILIDADES

Todos los empleados de Uriach, independientemente de su cargo, estarán obligados a cumplir las normas, procedimientos y controles establecidos para cumplir con la Normativa de PD aplicable.

El modelo de gobernanza para garantizar la buena actuación de Uriach en materia de protección de datos es:

- a) **Comité Global de Protección de Datos:** El Comité Global de Protección de Datos es el encargado de hacer efectiva la presente Política mediante la aplicación de las diferentes medidas previstas.

El Comité Global de Protección de Datos está compuesto, como miembros permanentes, por las personas físicas de Uriach que en cada momento ostenten el cargo de:

- Chief Legal & Sustainability Officer - Presidente
- Legal & Compliance Manager y DPO en HQ - Secretario
- Global Data & Technology Director - Miembro
- Cybersecurity Specialist - Miembro
- Global Digital & Data Director - Miembro

Se espera que los miembros del Comité Global de Protección de Datos mantengan un conocimiento actualizado de los requisitos legales y reglamentarios pertinentes, promuevan normativas adicionales que apliquen esta Política y proporcionen formación a todos los empleados.

- b) **Responsables locales de protección de datos:** Dependiendo de las necesidades locales y de la legislación aplicable, se pueden nombrar Responsables de Protección de Datos (RPD) locales y designarlos oficialmente ante las autoridades de control pertinentes. Estos RPD locales deben informar al Comité Global de Protección de Datos y son responsables de garantizar el cumplimiento de la normativa de protección de datos en sus respectivos territorios.
- c) **Miembros de la Organización:** Todos los miembros de la organización son responsables del cumplimiento de la normativa aplicable en materia de protección de datos y del correcto desarrollo de esta Política.

Todos los Miembros de la Organización, independientemente del cargo que ocupen, deberán velar por:

- garantizar el cumplimiento de las disposiciones de esta Política,
- responder inmediatamente a cualquier indicación que reciban del Comité Global de Protección de Datos, y

- consultar al Comité Global de Protección de Datos las dudas que puedan tener sobre la interpretación de esta Política o sobre la aplicación de la Normativa de Protección de Datos aplicable.

Asimismo, todos los Miembros de la Organización deberán notificar inmediatamente al Comité Global de Protección de Datos cualquier acción encaminada a prevenir o remediar la posible comisión de una infracción de la presente Política.

## **06 REGISTRO DE ACTIVIDADES DE TRATAMIENTO**

Cada empresa de Uriach implantará un Registro de Actividades de Tratamiento ("**RAT**"). Las operaciones de tratamiento incluidas en este RAT serán el resultado de un análisis realizado mediante entrevistas con todos los departamentos que puedan tratar datos personales en el desempeño de sus funciones.

El RAT se actualizará periódicamente para ofrecer una imagen actualizada del tratamiento realizado por cada empresa de Uriach.

## **07 DERECHOS DE LOS INTERESADOS**

Cada empresa de Uriach facilitará el ejercicio de los derechos de los interesados, ya sea cuando actúe como responsable del tratamiento o como encargado del tratamiento. Además, aplicarán normas, procedimientos o protocolos adecuados en relación con lo anterior.

## **08 CONTROL DE LOS PROVEEDORES**

El proceso de aprobación de los proveedores de Uriach incluirá una comprobación preliminar para confirmar, entre otras cosas, si el proveedor en cuestión requerirá el tratamiento de datos personales para prestar sus servicios o bienes.

Para ello, el control previo servirá para seleccionar a los proveedores y llevar a cabo un proceso previo de evaluación y homologación.

Cada empresa de Uriach podrá elaborar normas y procedimientos para desarrollar, concretar y detallar el contenido de este apartado. En particular, a título enunciativo y no limitativo, cada sociedad de Uriach utilizará únicamente encargados de tratamiento que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas, de tal forma que el tratamiento cumpla los requisitos de la Normativa aplicable en materia de PD y garantice la protección de los derechos de los interesados.

## **09 TRANSFERENCIAS INTERNACIONALES**

Uriach sólo transferirá datos personales a un tercer país o a una organización internacional fuera del Espacio Económico Europeo ("**EEE**") sobre la base de:

1. una decisión de adecuación;
2. garantías adecuadas, como las cláusulas contractuales tipo ("**CCT**");
3. normas corporativas vinculantes
4. una autorización de la autoridad de control competente; o
5. excepciones para situaciones específicas.

## **10 PERIODOS DE CONSERVACIÓN DE DATOS**

Las empresas Uriach almacenarán los datos personales de forma que sólo sea posible identificar a los interesados durante el tiempo necesario para los fines para los que se tratan los datos.

Las empresas elaborarán y actualizarán un esquema en el que se establezca el plazo de conservación de los datos que deban o consideren oportuno conservar de acuerdo con su respectiva Normativa de PD aplicable. En dicho esquema se considerarán los plazos de prescripción de las infracciones y las limitaciones establecidas en la Normativa de PD Aplicable, así como las obligaciones legales, sectoriales y contractuales que puedan requerir plazos de conservación superiores.

Las empresas de Uriach informarán a los interesados de los periodos de conservación cuando se recojan sus datos.

## **11 EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS ("EPID")**

Las empresas de Uriach evaluarán la necesidad de realizar una DPIA de acuerdo con sus respectivas normativas aplicables en materia de PD y, en caso necesario, la realizarán antes de que comience la actividad de tratamiento de datos pertinente.

## **12 RESPONSABLE DE LA PROTECCIÓN DE DATOS**

Cada empresa de Uriach llevará a cabo una evaluación de la necesidad de designar a un RPD de acuerdo con su respectiva Normativa de PD aplicable.

La necesidad de nombrar a un DPO se comunicará inmediatamente al Comité Global de Protección de Datos (dpo@uriach.com).

## **13 MEDIDAS DE SEGURIDAD**

Cada empresa de Uriach aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos. A estos efectos, cada organización deberá tener 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 el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

## **14 VIOLACIÓN DE DATOS Y COMUNICACIÓN DE RIESGOS**

Uriach implantará protocolos para hacer frente a las violaciones de datos y garantizar que se toman las medidas adecuadas, tanto preventivas como reactivas, y notificar cuando sea necesario a las autoridades de control competentes en un plazo de 72h y/o comunicar la violación a los interesados afectados.

Cualquier violación de los datos se comunicará inmediatamente al Comité Global de Protección de Datos.

## **15 AUDITORÍA DE PROTECCIÓN DE DATOS**

Uriach realizará auditorías periódicas para evaluar los riesgos a los que se refiere esta Política y garantizar el cumplimiento de su respectiva Normativa Aplicable en materia de PD.

Esta auditoría podrá ser interna, externa o mixta, e incluirá una verificación de la existencia, adecuación y eficacia de las medidas y controles establecidos para prevenir infracciones de las normas relativas a la protección de datos personales.

El alcance de esta auditoría diferirá del de la evaluación de impacto en que ésta se refiere a una operación de tratamiento específica, mientras que la auditoría de protección de datos se refiere al cumplimiento en toda la organización de la normativa aplicable en materia de protección de datos.

## **16 FORMACIÓN Y SENSIBILIZACIÓN**

Uriach promoverá la formación y sensibilización constante en materia de protección de datos a todos los niveles de la organización para mejorar la concienciación entre la organización en relación con la protección de datos de carácter personal.

Lo anterior se llevará a cabo tanto en sesiones presenciales como en cursos de e-learning o cualquier otro tipo de material y herramientas de comunicación y formación para concienciar de los riesgos de infracción a todos los niveles de la organización.

## **17 ACTUALIZACIÓN Y APLICACIÓN DE ESTA POLÍTICA**

La presente política y su aplicación se revisarán periódicamente. Cualquier modificación deberá ser aprobada por el CRC.

\*

\*

\*