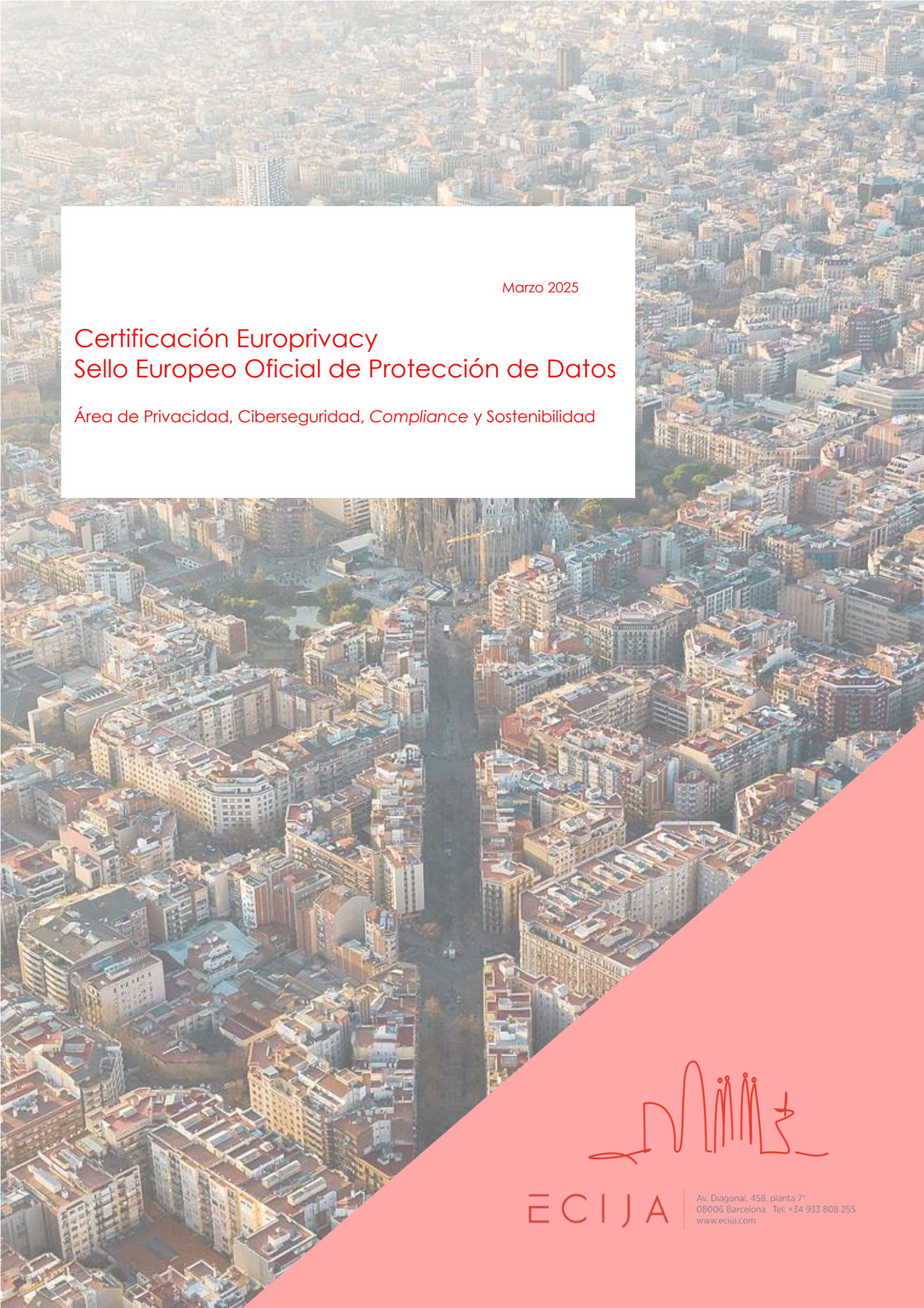

Marzo 2025

Certificación Europrivacy
Sello Europeo Oficial de Protección de Datos

Área de Privacidad, Ciberseguridad, *Compliance* y Sostenibilidad

ECIJA

Av. Diagonal, 458, planta 7ª
08006 Barcelona Tel: +34 933 808 255
www.ecija.com

Dossier informativo

Barcelona, Marzo 2025

Certificación Europrivacy[1]
Sello Europeo Oficial de Protección de Datos

Introducción

Europrivacy es un esquema de certificación diseñado para evaluar la conformidad de las operaciones de tratamiento de datos personales y **emitir certificaciones de cumplimiento** de acuerdo con el art. 42 del Reglamento General de Protección de Datos (RGPD).

Europrivacy ha sido aprobado oficialmente por el European Data Protection Board ("EDPB" o Comité Europeo de Protección de Datos), como el **primer Sello Europeo de Protección de Datos**[2], lo que ratifica su validez y aplicabilidad en todas las jurisdicciones de la UE y el EEE, así como la solidez de su metodología, basada en normas internacionales ISO.

El sistema se encuentra estrechamente alineado con los estándares internacionales de certificación, en particular con la ISO / IEC 17065 e ISO / IEC 17021-1, y su integración con estándares como ISO 27001 e ISO 27701 facilita sinergias con otros sistemas de gestión de la seguridad de la información, permitiendo la optimización de procesos y el refuerzo de las políticas de privacidad de forma integral en las organizaciones. Asimismo, Europrivacy puede extenderse a otras regulaciones complementarias y tecnologías emergentes.

Se trata de un **mecanismo voluntario** que permite a los responsables y encargados de tratamiento demostrar, de manera independiente e imparcial, que sus actividades de tratamiento cumplen con los requisitos exigibles en materia de protección de datos.

Contexto normativo y principales características

El RGPD establece en sus **artículos 42 y 43** la posibilidad de desarrollar **mecanismos de certificación** que constituyen una herramienta idónea para demostrar el cumplimiento normativo en materia de protección de datos. Permiten a las organizaciones, tanto en calidad de responsables como encargados del tratamiento, obtener una certificación que acredite la conformidad de sus actividades de tratamiento con los principios y requisitos del RGPD.

[1] Europrivacy es una marca internacional registrada en varias jurisdicciones. Más sobre Europrivacy: www.europrivacy.com

[2] Dictamen 28/2022 sobre los criterios de certificación de Europrivacy en cuanto a su aprobación por el Comité como Sello Europeo de Protección de Datos conforme al artículo 42, apartado 5 (RGPD) Adoptado | European Data Protection Board

Para asegurar la aplicación homogénea y efectiva de estos mecanismos en toda la Unión Europea, el **Comité Europeo de Protección de Datos** ha emitido diversas **directrices** que orientan sobre su implementación y supervisión. Entre las más destacadas se encuentran:

- **Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación conforme a los artículos 42 y 43 del RGPD**: Ofrecen una interpretación detallada de los requisitos para obtener la certificación, definiendo criterios y procedimientos para su implementación.
- **Directrices 4/2018 relativas a la acreditación de los organismos de certificación conforme al artículo 43 del RGPD**: Especifican los requisitos y criterios de acreditación para los organismos encargados de emitir certificaciones, garantizando así estándares uniformes en toda la UE.
- **Directrices 07/2022 sobre la certificación como herramienta para las transferencias internacionales de datos**: Detallan cómo la certificación puede ser utilizada para asegurar la conformidad con los requisitos en materia de transferencias de datos personales a terceros países o a organizaciones internacionales. Cabe destacar que, más allá de la mera obtención de un certificado, este tipo de mecanismos promueven una cultura de cumplimiento proactivo y transparencia, incentivando a las organizaciones a adoptar prácticas de protección de datos personales que superen el mínimo exigido por la normativa, en beneficio tanto de los ciudadanos como del desarrollo sostenible de la economía digital.

A quién está dirigida

La certificación Europrivacy está dirigida a aquellas entidades que realicen tratamientos de datos personales y deseen demostrar de forma transparente y verificable el cumplimiento del RGPD en relación con sus distintas actividades de tratamiento y, en su caso, con las obligaciones nacionales o sectoriales complementarias. En concreto, se dirige a:

- **Responsables y Encargados del tratamiento**. Organizaciones que gestionan datos personales y quieren evidenciar su conformidad mediante una evaluación independiente, establecidos en la Unión Europea y el Espacio Económico Europeo; si su empresa está situada fuera de esas jurisdicciones podemos informarle sobre Interprivacy ™/®[3]
- **Organizaciones de cualquier tamaño**. Aunque se presta una especial atención a aquellas entidades con un alto volumen de datos o que tratan información sensible, Europrivacy está abierta tanto a grandes corporaciones, como a PYMEs, siempre que cuenten con un Registro de Actividades de Tratamiento (RAT) y hayan designado un Delegado de Protección de Datos, puesto ambos requisitos son necesarios para obtener la certificación.
- **Entidades con actividades transversales**. Organizaciones que operan en diversos sectores y que deseen certificar no solo el cumplimiento del RGPD, sino la integración de controles específicos adaptados a su contexto particular ya sea por obligaciones nacionales o por el uso de tecnologías emergentes, como, por ejemplo, la Inteligencia Artificial (IA).
- **Organizaciones con interés en implementar tecnologías emergentes**. Aquellas que hacen uso de soluciones innovadoras como el Internet de las Cosas (IoT), la inteligencia artificial o blockchain, entre otras, y que requieren de un enfoque híbrido que combine criterios universales con controles complementarios específicos a sus riesgos y desafíos tecnológicos.

[3] https://www.interprivacy.org/index_es.html

Ventajas de la certificación

Evidencias de cumplimiento

En primer lugar, Europrivacy es un **medio para demostrar el cumplimiento normativo**, en tanto se fundamenta en las exigencias del RGPD y utiliza una metodología exhaustiva y verificada para asegurar que las actividades de tratamiento se alineen con la normativa de protección de datos personales. En este sentido, se generan indicios objetivos que validan el compromiso de una organización con la protección de datos, tales como:

- **Alineación normativa**. Europrivacy se basa en el artículo 42 RGPD, garantizando que cada evaluación esté en consonancia con los requisitos normativos establecidos, en este sentido, el sello certifica tratamientos de datos específicos, por tanto, la certificación no se lleva a cabo a nivel de compañía o de un sistema de gestión en su conjunto,
- **Metodología robusta y multidimensional**. Con el apoyo de distintos proyectos europeos, la metodología de certificación se despliega en base a un conjunto de 213 criterios y 659 requisitos, que permiten identificar de forma sistemática el nivel de cumplimiento.
- **Evaluación independiente**. La intervención de terceros cualificados asegura una valoración objetiva sin conflictos de interés.

Reputación y confianza

El segundo aspecto fundamental es la capacidad de Europrivacy para **fortalecer la reputación y la confianza tanto de los interesados como de socios comerciales y clientes**. Al contar con la aprobación del Comité Europeo de Protección de Datos y emitirse un sello – aprobado formalmente - de protección de datos, este mecanismo (i) certifica el cumplimiento y (ii) comunica de manera inmediata el compromiso con altos estándares de privacidad y seguridad, reforzando la credibilidad y el prestigio de las organizaciones certificadas.

Adaptabilidad y compatibilidad con otras certificaciones

El tercer pilar de relevancia radica en su capacidad para ofrecer un modelo innovador y flexible que se adapta a la complejidad del entorno digital actual, en el sentido de que ofrece:

- **Enfoque híbrido**. Combina criterios universales con controles complementarios específicos para sectores o tecnologías emergentes – como inteligencia artificial, IoT o blockchain.
- **Extensibilidad y flexibilidad**. Permite integrar obligaciones nacionales y adaptarse a marcos regulatorios complementarios, evitando duplicidades y optimizando la certificación.
- **Integración con estándares internacionales**. Su coherencia con normas internacionales facilita la combinación con otros esquemas (como ISO / IEC 27001 o 27701), potenciando la competitividad en el mercado global.
- **Innovación y actualización continua**. La incorporación de actualizaciones basadas en la evolución tecnológica y de los criterios de las autoridades de protección de datos, asegura que el esquema se mantenga relevante y a la vanguardia.

Diferencias con otras certificaciones de privacidad

En el contexto actual de la protección de datos, la existencia de diversos sistemas de certificación ha impulsado a las organizaciones a adoptar mecanismos que garanticen el cumplimiento normativo. En este sentido, el sello Europrivacy destaca por:

- **Reconocimiento oficial**. Cuenta con el reconocimiento oficial de Sello Europeo de Protección de Datos y la aprobación del CEPD. Este reconocimiento garantiza que la certificación se aplique de manera uniforme en toda la UE y EEE, en base al cumplimiento de los requisitos del RGPD.
- **Enfoque proactivo**. Europrivacy no consiste en un mero trámite de verificación normativa, sino que busca incentivar a las organizaciones de manera activa en la cultura de la privacidad.
- **Aplicabilidad y alcance territorial**. Debido a su carácter europeo y a la alineación con las directrices del EDPB, Europrivacy ostenta validez y aplicabilidad uniforme en todas las jurisdicciones de la UE y EEE, de lo que resulta un enfoque altamente beneficioso para organizaciones con operaciones transfronterizas.
- **Criterio a tener en cuenta en la imposición de sanciones**. El artículo 83.2 del RGPD dispone que al decidir la imposición de una multa administrativa y su cuantía, entre otras cuestiones, se tendrá en cuenta la adhesión a mecanismos de certificación aprobados con arreglo al artículo 42 del RGPD.

Alcance de la certificación

El alcance de la certificación Europrivacy es definido por la organización, la cual deberá establecer las actividades de tratamiento que quiere que sean objeto de evaluación y certificación.

Para obtener la certificación, la organización debe contar con una estructura mínima que incluya la **figura del Delegado de Protección de Datos** (DPD), sea interno o externo. Este requisito es fundamental para asegurar la capacidad interna necesaria para monitorizar y mantener el cumplimiento normativo; además, deberá disponer de un Registro de Actividades de Tratamiento (RAT).

Es importante señalar que existen **dominios de aplicación excluidos de la certificación** regular (por ejemplo, el tratamiento de información genética), en el sentido de que estén sujetos a obligaciones específicas que varían significativamente según la legislación nacional; para evitar interpretaciones erróneas, Europrivacy mantiene una lista actualizada de ámbitos excluidos del alcance estándar del esquema.

Proceso de implementación, certificación y mantenimiento

Implementación y certificación

El proceso para obtener la certificación **Europrivacy** sigue un enfoque sistemático que garantiza la evaluación y validación independiente del cumplimiento normativo, los pasos principales son:

- **Solicitud de certificación**: La organización debe completar el Formulario de Aplicación Europrivacy, en el cual se detalla el alcance del tratamiento a certificar.
- **Revisión inicial de la solicitud**: El organismo certificador verifica que la solicitud y el alcance cumplen con los requisitos del esquema y las directrices del EDPB.

- **Evaluación de conformidad**: Se realiza una auditoría formal en la que un auditor independiente revisa la documentación, políticas, procesos y medidas de seguridad aplicadas al tratamiento de datos.
- **Identificación de no conformidades**: Si se detectan no conformidades, estas se clasifican como menores o mayores, y se proporciona un plazo para corregirlas.
- **Informe final del auditor**: Una vez corregidas las no conformidades, se elabora un informe final en el que se valida el cumplimiento del tratamiento de datos con los requisitos del esquema Europrivacy.
- **Decisión de certificación**: El organismo certificador revisa el informe y, si se cumplen los requisitos, emite la certificación Europrivacy.
- **Publicación del certificado**: La certificación es registrada y publicada en el **Registro Europrivacy de Certificados**, lo que permite su validación y reconocimiento a nivel europeo.

Mantenimiento y renovación de la certificación

Para garantizar la continuidad de la certificación Europrivacy, las organizaciones deben cumplir con un proceso de mantenimiento y renovación que consta de las siguientes fases:

- **Mantenimiento de la conformidad**: la organización debe asegurarse de que el tratamiento de datos certificado sigue cumpliendo con los criterios de certificación y con cualquier actualización normativa.
- **Auditorías de supervisión**: se realizan auditorías de vigilancia anuales para verificar el cumplimiento continuo. Estas auditorías deben llevarse a cabo:
  - **Primera auditoría de vigilancia**: dentro de los 12 meses posteriores a la certificación.
  - **Segunda auditoría de vigilancia**: dentro de los 24 meses posteriores a la certificación.
- **Revisión ante cambios normativos u organizativos**: si se producen cambios significativos en las regulaciones aplicables, la organización debe actualizar su documentación y garantizar el cumplimiento con los nuevos requisitos.
- **Renovación de la certificación**: la certificación tiene una validez de tres años. Antes de su vencimiento, la organización debe someterse a un proceso de recertificación, que implica una auditoría similar a la inicial para evaluar el cumplimiento continuo con el esquema Europrivacy.

Este proceso garantiza que la certificación siga siendo válida y confiable, asegurando que las organizaciones mantengan los estándares más altos en materia de protección de datos.

Recomendaciones y recursos de referencia

Para optimizar el proceso de certificación **Europrivacy**, se recomienda realizar una **autoevaluación previa**, definir claramente el **tratamiento que se quiere certificar**, mantener una **documentación actualizada**, y apoyarse en expertos en **protección de datos**. Además, es clave mantenerse informado sobre cambios normativos y preparar auditorías de supervisión para garantizar la continuidad del cumplimiento.

Algunos recursos útiles para conocer más sobre Europrivacy incluyen la **Comunidad Europrivacy,** con acceso a guías y plantillas, **la página web oficial de Europrivacy** con información sobre certificación, y el **Comité Europeo de Protección de Datos (CEPD)** con directrices actualizadas.

ECIJA, después de pasar el correspondiente proceso de aprobación de su condición de Colaborador Oficial de Europrivacy, por parte de la entidad que gestiona Europrivacy, es un socio experto a nivel global[4], lo que implica que **dispone de profesionales certificados para llevar a cabo las tareas necesarias para implementar el mecanismo de certificación, acompañando a las empresas de manera eficaz en el proceso de obtención del sello**.

Para más información sobre Europrivacy, contacte con europrivacy@ecijalegal.com

_____

Departamento de Privacidad, Compliance, Ciberseguridad y Sostenibilidad
Ecija Barcelona
T +34 933 808 255
info@ecijalegal.com
https://www.ecija.com

[4] https://www.europrivacy.org/es/partners/list