



WEBINAR

Protección de datos y empresas fintech



EVA ESTEVEZ

Abogada y DPO

Asesora legal experta en
protección de datos y
Máster en compliance penal.



ANDREA GONZÁLEZ

Asesora legal

Especialista en protección
de datos, postgrado en
derecho privado europeo



**¡Envíanos tus
preguntas!**

eva.estevez@pridatect.com

andrea.gonzalez@pridatect.com

01. Introducción: empresas fintech y RGPD



El fintech se refiere a la integración de la tecnológicas con los servicios financieros. Banca, empresas vinculadas al sector seguros o inversiones y startups enfocadas en realizar pagos y transacciones, entre otras, se han hecho eco de lo que ya supone una revolución en el sector.



El fintech permite que los usuarios puedan hacer diferentes operaciones a través del móvil. Está en pleno crecimiento y en unos años posiblemente supere al del número de usuarios de empresas financieras tradicionales.



El fintech requiere la utilización de diferentes datos de los usuarios, por lo tanto, adaptarse al RGPD y **garantizar la mayor seguridad** es un aspecto primordial para este tipo de empresas.



02. Contenidos



Cómo afecta el RGPD en el sector fintech



¿Qué se puede hacer con los datos de los usuarios?



Identificación de clientes



Compartir datos con terceros

Comunicar brechas de seguridad

03. Cómo afecta el RGPD en el sector fintech: la importancia de la protección de datos



Para poder realizar gestiones como pedir un préstamo o una hipoteca online se requiere determinada información y datos sensibles. Una fintech puede llegar a tomar muchas decisiones basándose en datos, lo que supone contar con unas medidas especiales para la autenticación, y el obligado cumplimiento de los siguientes puntos del RGPD:

- Respetar el principio de exactitud de los datos, el de licitud del tratamiento y el de consentimiento informado, así como garantizar todas las medidas de seguridad necesarias en los procesos de identificación.
- Garantizar el derecho a no ser objeto de decisiones automatizadas.
- Tener un correcto protocolo de comunicación de brechas de seguridad
- Establecer las medidas técnicas y organizativas necesarias para las gestiones con terceros.

“Las fintechs utilizan datos que permiten tomar decisiones crediticias, administrar riesgos y analizar fraudes, lo que da pie a estar tratando con información muy sensible”

03. 1 Cómo afecta el RGPD en el sector fintech: qué podría ocurrir con el uso fraudulento de datos



El mundo digital está en constante cambio y crece rápidamente, lo que supone un reto para empresas del sector financiero que quieren unirse a las posibilidades que la tecnología les puede brindar.

- Los cambios tecnológicos no pueden dejar brechas en los sistemas de seguridad de una empresa fintech, aspecto que trata de tener bajo control la AEPD.
- Las implicaciones que podría tener un uso fraudulento de los datos: suplantación de identidad, etc.

Ejemplo de entidad financiera que sufrió una suplantación de identidad



Fueron tratados los datos personales de una persona sin su consentimiento, realizándose la petición de un crédito e incluyendo sus datos en un fichero de solvencia.

“La AEPD (Agencia Española de Protección de Datos) ha cuestionado en varias ocasiones las medidas de seguridad a la hora de identificar a los clientes en el sector fintech, ya que es algo primordial para evitar fraudes”

04. ¿Qué se puede hacer con los datos de los usuarios?



Es muy importante ser transparente a la hora de informar sobre el uso que se le va a dar a los datos y cumplir con los siguientes requerimientos:

- Obtener el consentimiento informado
- Las decisiones que se tomen mediante herramientas automatizadas tienen que ser justas e imparciales.
- Los datos que se utilizan tienen que ser precisos, no se debe pedir más datos de los estrictamente necesarios y estos se tienen que utilizar únicamente de forma justificada.
- El RGPD fomenta y controla el uso de la **seudonimización**, ya que se pueden reducir los riesgos.

“El RGPD indica que para que sea válido el consentimiento del cliente, este tiene que ser específico, informado e inequívoco”



05. Identificación de clientes: medidas para evitar la suplantación de identidad

La suplantación de la identidad es uno de los mayores fraudes con los que una fintech o usuario de fintech se puede ver afectados, por lo tanto, garantizar las mayores medidas de seguridad es uno de los aspectos en los que más habría que incidir para garantizar la protección de los datos.

La doble autenticación garantiza una mayor seguridad.



Establecer unas medidas adecuadas para garantizar la privacidad de los datos personales



KYC (Know Your Customer) y AML (prevención de blanqueo de capitales) agrupan los requerimientos que una empresa financiera tiene que realizar para verificar la identidad de sus clientes



05. 1. Identificación de clientes: la firma electrónica



La firma electrónica permite operar con mayor rapidez en las fintech y en muchos casos los usuarios se plantean si son seguras. Permite realizar operaciones de forma segura gracias a eIDAS, lo que supone una **ventaja para el sector fintech** gracias a sus requerimientos:

- Tiene que dar información de identificación única vinculada a la de la persona que firma.
- La persona que realiza la firma tiene completo control de los datos utilizados para crear dicha firma electrónica.
- La firma electrónica tiene que poder identificar si los datos que acompañan el mensaje han sido manipulados después de haber sido firmados. Si los datos firmados han cambiado, la firma se marcaría como no válida.
- Hay un certificado de firma electrónica, prueba electrónica que confirma la identidad del firmante y vincula los datos de validación de la firma electrónica a esa persona.

“eIDAS (electronic IDentification, Authentication and trust Services) es el reglamento europeo de reconocimiento de identidades electrónicas para la identificación electrónica y los servicios de confianza para transacciones electrónicas”

05. 2 Datos biométricos



Los datos biométricos, como la autenticación facial o las huellas dactilares, son una de las principales formas de identificación de clientes en el sector fintech.

- Es necesario contar con el consentimiento explícito del interesado para obtener estos datos biométricos.
- Para cumplir con el RGPD es necesario establecer una serie de medidas técnicas y organizativas para evitar que estos datos sufran algún riesgo.

“El RGPD define los datos biométricos como aquellos que son relativos a las características físicas, fisiológicas o conductuales de una persona, y considera que necesitan ser tratados como datos sensibles”

06. Compartir datos con terceros



Los datos de los clientes se suelen compartir con distintas aplicaciones que pueden ser subcontratadas por una fintech. Esto expone los datos personales, por lo tanto, el RGPD exige determinadas obligaciones y responsabilidades para ambas empresas.

Cuando se comparten estos datos es necesario establecer un contrato y tener en cuenta las siguientes obligaciones:

El responsable de tratamiento de los datos tiene que tener en cuenta el deber de información y el de atención de derechos de rectificación, cancelación y oposición.

- Legitimación
- Obligación de informar
- Derechos de rectificación y cancelación
- Derech de oposición

El tercero, no sería el responsable, pero tiene que estar informado cuando el usuario o cliente pida hacer algún cambio:



07. Las brechas de seguridad en el sector fintech



La seguridad es uno de los grandes retos para las empresas fintech. Tener un protocolo de gestión y comunicación de brechas de seguridad es un aspecto imprescindible.

- Para una fintech es fundamental establecer medidas preventivas que eviten errores humanos o errores informáticos o del sistema utilizado, ya que estos son los principales aspectos que pueden ocasionar una brecha de seguridad.
- Estar preparado ante los posibles ataques de hackers o robo de datos y contar con un plan de actuación puede evitar grandes daños en seguridad y reputación.

“Ante una brecha de seguridad, la empresa tendría la obligación de comunicársela inmediatamente al AEPD y a los clientes, usuarios o personas afectadas-”

Pridatect, plataforma para simplificar el proceso de identificar riesgos y proteger datos



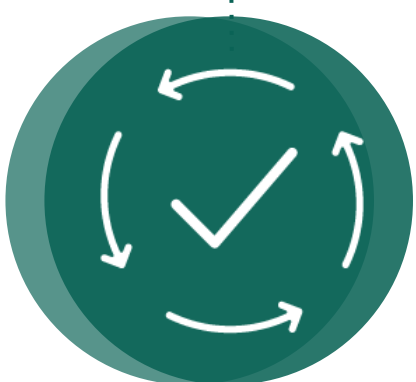
DETECTAR E IDENTIFICAR RIESGOS

Detecta e identifica los riesgos en tu tratamiento de datos personales (**clientes, empleados, proveedores...**). Con la plataforma de Pridatect podemos identificar y analizar, las amenazas y vulnerabilidades en tus procesos.



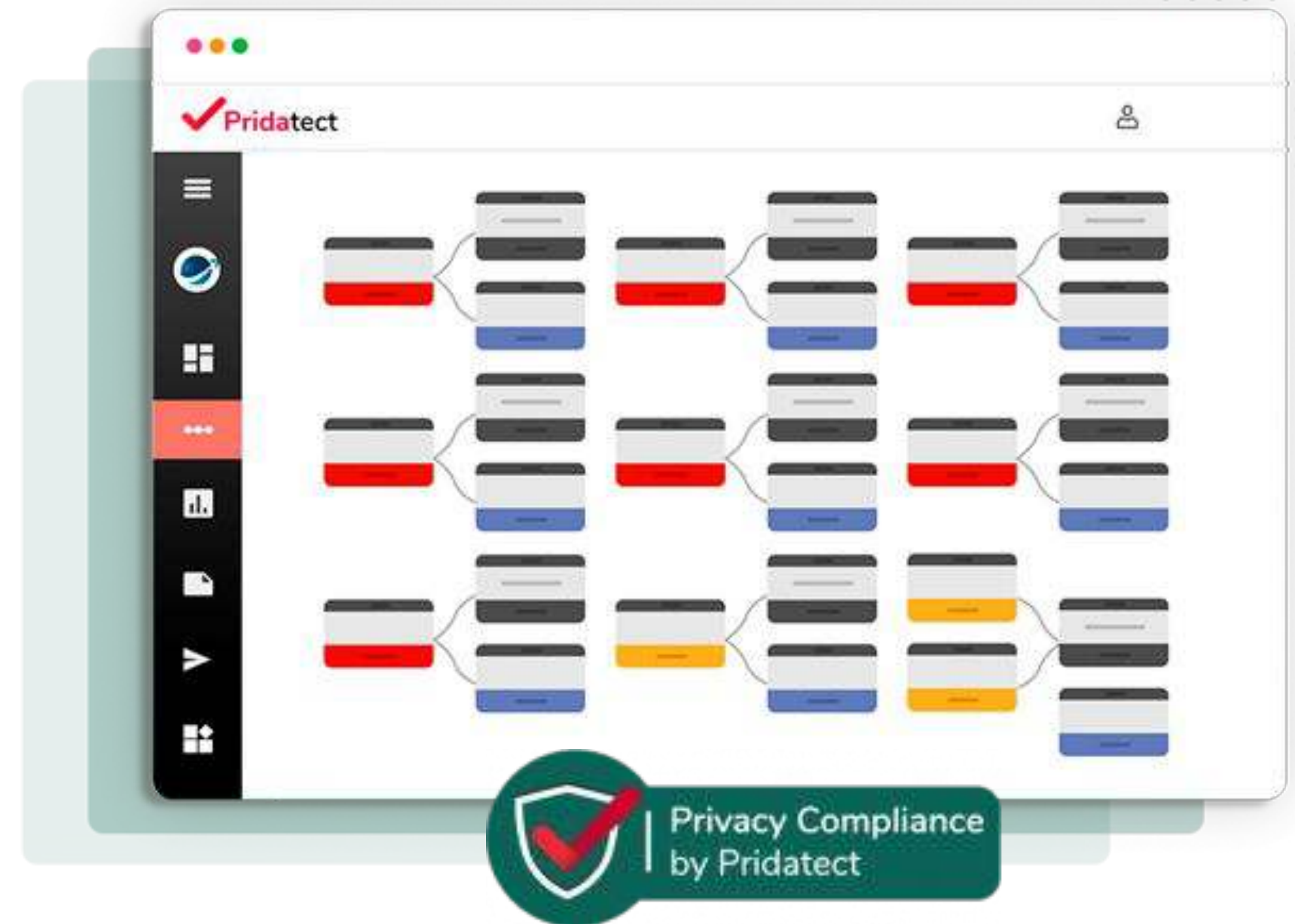
DEFINIR Y SUGERIR MEDIDAS

El conocimiento de los riesgos en tu empresa nos permite definir las medidas necesarias para reducirlos y mitigarlos. Pridatect te ayuda con la definición y sugerencias de medidas para tu empresa.



SUPERVISIÓN E IMPLEMENTACIÓN DEL PROGRAMA

La protección de datos es una tarea constante dentro una empresa. Pridatect no solo ayuda con la implementación inicial, también con la supervisión continua de riesgos, medidas y administración de tareas entre empleados de tu empresa.



Solución tecnológica de confianza para tu protección de datos

Todo lo que necesitas para cumplir con el RGPD



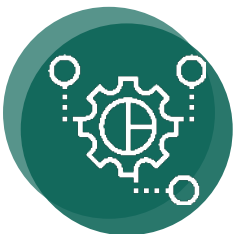
Evaluación de riesgos

Elimina riesgos de datos



Evaluación de impacto

Evaluación de impacto automatizada



Análisis de cumplimiento

Identifica brechas en tu protección de datos



Actividades de tratamiento

Ten un registro de actividades de tratamiento actualizado



Mapa de datos

Mapea los flujos de datos de tu empresa



TOMs

Define medidas técnicas y organizativas para reducir el riesgo



Informes de privacidad

Genera informes de privacidad automáticamente



Transferencias internacionales

Gestiona transferencias internacionales de datos



Gestión brechas de seguridad

Maneja exitosamente las brechas de seguridad



Cumplimiento de tu web

Genera políticas de privacidad, políticas de cookies, términos y condiciones



Derechos ARCO

Gestiona las peticiones de derechos de accesos y sujetos



Userdesk cloud seguro

Entorno cloud colaborativo y 100% seguro



Servicio DPO externo

DPO Virtual para tu empresa



Contratos con proveedores

Genera los contratos que necesitas por el RGPD



Automatización de documentos

Crea documentos legales basados en nuestros modelos

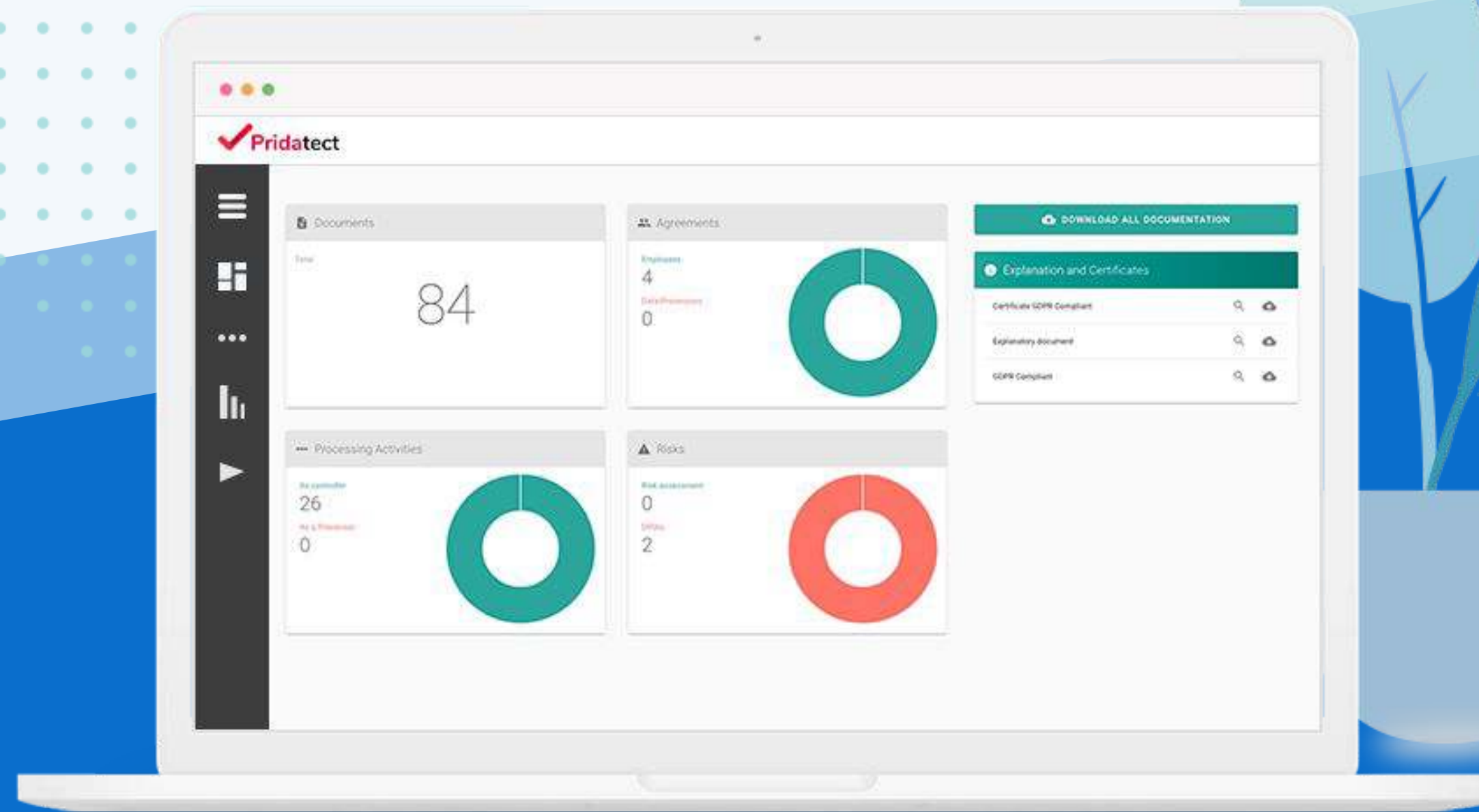
¡Haz la prueba con Pridatect!



Toma el control de la gestión de la protección de datos de empresa y garantiza el cumplimiento del RGPD, ofreciendo la mayor seguridad a tus clientes. En Pridatect te ayudamos a detectar riesgos y a tomar las medidas adecuadas.

Solicita tu demo
gratuita

Contacta con nosotros para una [demo gratuita](#) o utiliza nuestra [prueba gratuita](#) durante 7 días.



¡Gracias por ver
nuestro Webinar!