Fiwy

Políticas de privacidad

Índice

Vista de Privacidad de Datos, Seguridad y Cumplimiento

1 Introducción

En Fivvy, damos prioridad a la privacidad y seguridad de los datos que recopilamos y procesamos. Como una plataforma de inteligencia empresarial impulsada por IA, operamos en pleno cumplimiento con los requisitos regulatorios de diversas jurisdicciones, incluidos los principales mercados de aplicaciones globales como Google Play Store y Apple App Store. Este documento ofrece una visión detallada de cómo garantizamos la anonimización, seguridad y compatibilidad de los datos con diferentes ecosistemas regulatorios, respaldados por nuestra sólida infraestructura construida sobre Amazon Web Services (AWS).

2 Recopilación de Datos: Garantizando la Anonimidad

En el núcleo del proceso de recopilación de datos de Fivvy se encuentra el enfoque en mantener el anonimato mientras se proporcionan conocimientos valiosos y procesables. Logramos esto recopilando datos a través de las aplicaciones móviles de nuestros clientes, centrándonos en identificadores a nivel de dispositivo, como el ID de dispositivo. Este método asegura que Fivvy nunca capture ni almacene información personal identificable (PII), como nombres, direcciones de correo electrónico o números de teléfono. La siguiente sección ofrece una explicación detallada de cómo se obtiene y utiliza el ID de dispositivo dentro de nuestro sistema para mantener la privacidad mientras entregamos insights de alto valor.

3 Obtención del ID de Dispositivo

El ID de dispositivo es un identificador único alfanumérico asignado a cada smartphone o dispositivo móvil por el sistema operativo del mismo. Este identificador es utilizado por los desarrolladores de aplicaciones para reconocer los dispositivos que han instalado su app sin acceder a ningún dato específico del usuario. A continuación, se detalla el proceso técnico involucrado en la obtención y utilización del ID de dispositivo:

4 Instalación de la Aplicación y Permisos

Cuando un usuario descarga e instala la aplicación móvil de un cliente, la app solicita permisos específicos al usuario para recopilar ciertos tipos de datos. Estos permisos generalmente incluyen acceso básico al ID de Dispositivo y otros metadatos anonimizados. Es importante destacar que la obtención del ID de Dispositivo se realiza en estricto cumplimiento con las políticas de privacidad de la tienda de aplicaciones y los marcos de consentimiento del usuario (por ejemplo, solicitudes de consentimiento compatibles con el RGPD en la UE).

Consentimiento del Usuario

La aplicación presenta un cuadro de diálogo claro y transparente a los usuarios, detallando los datos que se recopilan (como el ID de Dispositivo) y cómo se utilizarán. Los usuarios deben otorgar su consentimiento explícito, garantizando el cumplimiento con las regulaciones de

privacidad globales.

Identificación del Dispositivo

Tras otorgar su consentimiento, la aplicación móvil extrae el ID de Dispositivo del sistema operativo (como el ID de Publicidad de Android o el Identificador para Anunciantes de Apple - IDFA). Estos identificadores están estandarizados en los ecosistemas móviles para permitir el seguimiento de publicidad y análisis sin involucrar datos personales

5 Recolección de Datos a Nivel de Dispositivos

Fivvy utiliza el identificador de dispositivo (device ID) para rastrear y analizar comportamientos específicos del dispositivo. Esto nos permite optimizar la experiencia del usuario y obtener insights valiosos sobre el uso de aplicaciones. Entre la información recolectada se incluye:

- ✓ Tiempo dedicado a diversas aplicaciones.
- ✓ Interacción con aplicaciones de la competencia (por ejemplo, qué aplicaciones de competidores utiliza el usuario).
- ✓ Métricas de rendimiento de la aplicación, como tiempos de carga, errores y frecuencia de uso.

De acuerdo con la legislación aplicable, se consideran datos personales aquellos relativos a cualquier información concerniente a personas naturales, ya sean identificadas o identificables (en adelante, "Datos Personales"). Por ello, Fivvy se compromete a manejar esta información de manera transparente y segura, cumpliendo con normativas como el GDPR y otras regulaciones vigentes.

Para procesar aquellos datos que sean considerados sensibles, Fivvy solicitará el consentimiento expreso del usuario final. Entre los datos que se recopilan se encuentran:

- ✓ **Número de identificador del dispositivo (device ID) y dirección IP:** Utilizados exclusivamente para atribución y análisis estadístico.
- ✓ **Información estadística de uso del dispositivo:** Basada en un listado específico y predefinido de aplicaciones.
- ✓ **Lista predefinida de aplicaciones:** Que permite establecer un marco de referencia para el análisis del comportamiento del usuario.
- ✓ **Datos y metadatos adicionales:** Que posibilitan la construcción y/o reconstrucción total del uso de las aplicaciones, incluyendo el tiempo de uso, sin llegar a comprometer la identidad del usuario.

Este enfoque asegura que el tratamiento de los Datos Personales se realice de forma responsable y conforme a la normativa, protegiendo la privacidad de los usuarios en cada etapa del procesamiento.

Propósitos de la recolección de información

Esta herramienta dinámica sirve al cliente como base para:

- ✓ Mejorar las estrategias de marketing.
- ✓ Lograr políticas de segmentación y retención de clientes
- ✓ Comprender en tiempo real las nuevas tendencias de comportamiento y consumo.
- ✓ Mejorar las oportunidades de venta.
- ✓ Análisis de la competencia para mejorar el posicionamiento en el mercado.
- ✓ Evaluar, monitorear y mejorar los servicios, midiendo, analizando y entendiendo a los usuarios de la Aplicación Móvil, y el desempeño y la utilización de plataformas, así como los hábitos de navegación de los usuarios.
- ✓ Desarrollar, materializar e implementar acciones comerciales, tales como acuerdos comerciales o alianzas con terceros, así como la implementación de soluciones de publicidad en línea.

6 El rol del ID de Dispositivo Anónimo en los Insights Accionables

Al aprovechar el ID de Dispositivo anónimo, Fivvy permite a las empresas obtener potentes insights a nivel de dispositivo sin infringir la privacidad del usuario. Así es como funciona en la práctica:

Seguimiento de Interacciones sin PII: El ID de Dispositivo proporciona a nuestros clientes información valiosa sobre cómo los usuarios interactúan con sus aplicaciones. Esto incluye patrones de comportamiento como la duración de las sesiones, la frecuencia de uso de la aplicación y la interacción con aplicaciones de la competencia. Todo esto se logra sin recopilar información personal.

Mapeo del ID de Dispositivo con Datos de Clientes: Nuestros clientes pueden individualizar aún más los insights generados por Fivvy mapeando el ID de Dispositivo anónimo con sus propios IDs de clientes internos. Aunque Fivvy no tiene conocimiento de la identidad específica del usuario, los clientes que gestionan sus propias bases de datos de clientes pueden correlacionar el ID de Dispositivo con sus registros internos. Esto permite a los clientes:

- ✓ Identificar usuarios de alto valor basándose en el comportamiento del dispositivo.
- ✓ Desarrollar campañas de marketing altamente segmentadas (por ejemplo, ofreciendo promociones especiales a usuarios frecuentes de una app de la competencia).
- ✓ Tomar decisiones basadas en insights en tiempo real a nivel de dispositivo, mientras se preserva el anonimato del usuario dentro del ecosistema de Fivvy.

Esto garantiza que los datos sean accionables y relevantes, cumpliendo al mismo tiempo con las regulaciones de privacidad.

7 Anonimato y Cumplimiento Normativo

El uso del Device ID por parte de Fivvy cumple con los marcos regulatorios globales, incluyendo el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, la Ley de Privacidad del Consumidor de California (CCPA) en los Estados Unidos y otras normativas de privacidad relevantes.

Cumplimiento con el GDPR

Según el GDPR, los Device IDs se clasifican como datos seudónimos, lo que significa que, aunque están vinculados a un dispositivo específico, no pueden atribuirse fácilmente a una persona específica. Fivvy procesa los Device IDs de manera que cumple con los requisitos del GDPR, asegurando que los datos se recopilen con el consentimiento del usuario y se procesen de forma minimizada y segura.

Cumplimiento con el CCPA

El CCPA clasifica ciertos datos a nivel de dispositivo, incluido el Device ID, como "información personal" si pueden vincularse a un individuo. Fivvy garantiza que los datos permanezcan completamente anónimos y no se utilicen para identificar a ninguna persona, cumpliendo con los estándares del CCPA.

8 El Device ID en el Marco General de Seguridad

El Device ID anónimo forma parte de la arquitectura de seguridad más amplia de Fivvy, diseñada para garantizar que todos los datos recopilados se manejen de la manera más segura y conforme posible. Utilizamos Amazon Web Services (AWS) para procesar, almacenar y analizar los datos en un entorno seguro, con cifrado estándar de la industria y políticas de control de acceso implementadas.

Cifrado

Todos los datos, incluidos los Device IDs, están cifrados tanto en reposo como en tránsito, lo que garantiza que, incluso si los datos fueran interceptados, permanecerían ilegibles y seguros.

Control de Acceso

Fivvy implementa estrictas políticas de control de acceso basado en roles (RBAC), asegurando que solo el personal autorizado pueda acceder a datos sensibles y únicamente para propósitos específicos alineados con los principios de privacidad establecidos.

Cumplimiento normativo

La recopilación y procesamiento de datos de Fivvy cumple completamente con el Reglamento General de Protección de Datos (GDPR), la Ley de Privacidad del Consumidor de California (CCPA) y otras regulaciones de privacidad regionales. Estos marcos garantizan que se respeten los derechos de los individuos sobre sus datos mientras se permite a las empresas obtener conocimientos significativos.

1 Reglamento General de Protección de Datos (GDPR)

El GDPR es una ley integral de privacidad que se aplica a las empresas que procesan los datos personales de ciudadanos de la Unión Europea. Esta legislación fue diseñada para otorgar a los individuos un mayor control sobre sus datos personales y garantizar la transparencia y seguridad en cómo las organizaciones manejan dicha información.

Principios clave del GDPR

- ✓ **Minimización de datos:** Solo deben recopilarse los datos necesarios para el propósito previsto.
- ✓ **Transparencia:** Las organizaciones deben comunicar claramente cómo se recopilan, procesan y utilizan los datos personales.
- ✓ **Consentimiento del usuario:** Se debe obtener el consentimiento de los usuarios antes de recopilar o procesar sus datos personales, y los usuarios tienen el derecho de retirar dicho consentimiento en cualquier momento.
- ✓ **Derecho de supresión ("Derecho al olvido"):** Los usuarios pueden solicitar que sus datos personales sean eliminados bajo ciertas condiciones.
- ✓ **Portabilidad de datos:** Los usuarios tienen derecho a recibir sus datos en un formato portátil o transferirlos a otro proveedor de servicios.

2 Ley de Privacidad del Consumidor de California (CCPA)

La CCPA es una ley de privacidad similar que se aplica a las empresas que operan en California o manejan los datos personales de residentes de California. Proporciona a los consumidores el derecho de saber qué información personal se está recopilando sobre ellos y cómo se está utilizando.

Características clave de la CCPA

- ✓ **Derecho de Acceso:** Los consumidores pueden solicitar detalles sobre qué datos personales se están recopilando sobre ellos.
- ✓ **Derecho a Rechazar:** Los usuarios pueden optar por excluirse de la venta de sus datos personales.

- **Derecho a la Eliminación:** Similar al GDPR, los consumidores pueden solicitar que sus datos personales sean eliminados.
- **No Discriminación:** Las empresas no pueden discriminar a los usuarios que ejerzan sus derechos de privacidad (por ejemplo, ofreciendo un servicio de menor calidad).

3 Qué deben hacer las empresas para cumplir con las normativas

Para cumplir con el GDPR, CCPA y otras regulaciones de privacidad, las empresas deben seguir procedimientos específicos al recopilar y procesar datos. Las acciones clave requeridas incluyen:

✓ Obtención del consentimiento del usuario

Para que las empresas puedan recopilar datos, deben obtener el consentimiento explícito de los usuarios, informándolos de manera clara sobre qué datos se están recopilando, cómo se utilizarán y por qué. Para las empresas que utilizan aplicaciones móviles, esto a menudo implica presentar a los usuarios un cuadro de diálogo de consentimiento que cumpla con los requisitos de las tiendas de aplicaciones (por ejemplo, Google Play Store o Apple App Store), donde se explique el uso de datos como los ID de dispositivo y los patrones de comportamiento.

✓ Minimización de datos

Las empresas deben recopilar únicamente los datos necesarios para sus servicios. Esto implica evitar la recopilación excesiva de datos que podría considerarse innecesaria según el principio de minimización de datos del GDPR. Por ejemplo, recopilar únicamente el ID del dispositivo y datos de uso anonimizados, sin información personal, ayuda a reducir el riesgo regulatorio.

✓ Solicitudes de acceso y eliminación de datos por parte de los usuarios

Las empresas deben contar con sistemas que permitan a los usuarios acceder a los datos recopilados sobre ellos y solicitar su eliminación. Para las aplicaciones móviles, esto podría implicar ofrecer una forma sencilla para que los usuarios gestionen sus datos dentro de la app o a través del servicio de atención al cliente.

✓ Notificaciones de violación de datos

En caso de una violación de datos, las empresas deben notificar a los usuarios afectados y a las autoridades regulatorias dentro de un período de tiempo específico (72 horas según el RGPD).

4 El Rol de Fivvy en Garantizar el Cumplimiento

La plataforma de Fivvy está diseñada para apoyar a las empresas en sus esfuerzos por cumplir con estas regulaciones de privacidad, facilitando el cumplimiento de los requisitos regulatorios sin sacrificar información valiosa. A continuación, se detalla cómo Fivvy garantiza el cumplimiento y ayuda a sus clientes a evitar problemas regulatorios:

Recopilación de Datos Anónimos

Fivvy recopila únicamente datos anónimos vinculados a los ID de dispositivos, asegurando que nunca se capture información personal (por ejemplo, nombres, direcciones de correo electrónico o números de teléfono). Estos datos incluyen patrones de uso de aplicaciones, tiempo de uso y tipo de dispositivo, todos asociados a ID de dispositivos anónimos en lugar de usuarios identificables. Al trabajar exclusivamente con datos anonimizados, ayudamos a reducir la carga del cumplimiento de GDPR y CCPA para nuestros clientes, ya que en nuestra plataforma no se almacenan ni procesan datos personales.

Gestión de Consentimiento

Nuestra plataforma opera en total cumplimiento con los requisitos de consentimiento establecidos por el GDPR y la CCPA. Cuando un usuario instala una aplicación integrada con Fivvy, la aplicación debe mostrar una solicitud de consentimiento al usuario antes de que comience cualquier recolección de datos. Esto garantiza que los usuarios estén informados y hayan dado su consentimiento explícito, cumpliendo con las obligaciones de transparencia y consentimiento establecidas tanto por el GDPR como por la CCPA. Trabajamos con nuestros clientes para asegurar que sus diálogos de consentimiento cumplan con las normativas y reflejen prácticas precisas de uso de datos.

Acceso y Portabilidad de Datos

Fivvy apoya a las empresas en la gestión de los derechos de los sujetos de datos bajo el GDPR y la CCPA. Aunque la plataforma de Fivvy no almacena información personal, proporcionamos herramientas para que nuestros clientes gestionen solicitudes de usuarios que deseen acceder o eliminar los datos anonimizados asociados con su Device ID. Dado que solo manejamos datos anónimos, este proceso es eficiente, ya que no tratamos información sensible o identificable personalmente.

Cumplimiento en las Tiendas de Aplicaciones

Fivvy garantiza que las prácticas de recopilación de datos de las aplicaciones que utilizan nuestra tecnología cumplan con las políticas de Google Play Store y Apple App Store. Trabajamos en estrecha colaboración con nuestros clientes para asegurar que sus aplicaciones sigan las estrictas directrices de las tiendas de aplicaciones, como obtener el consentimiento del usuario para la recopilación de datos, adherirse a las políticas de privacidad y utilizar permisos estándar de las aplicaciones.

5 Lo que las empresas necesitan hacer para mantener el cumplimiento

Para las empresas que utilizan la plataforma de Fivvy, el cumplimiento de normativas como el GDPR y la CCPA sigue siendo una responsabilidad compartida. A continuación, se presentan los pasos que las empresas deben seguir:

Revisar y actualizar las políticas de privacidad

Las empresas deben mantener sus políticas de privacidad actualizadas, explicando claramente el uso de la plataforma de Fivvy y cómo se recopilan y procesan los datos anónimos a nivel de dispositivo. Esta transparencia es fundamental para cumplir con los requisitos de notificación establecidos por el GDPR y la CCPA.

Mantener mecanismos de consentimiento

Las empresas deben garantizar que cuentan con mecanismos de consentimiento efectivos dentro de sus aplicaciones móviles. Esto incluye proporcionar opciones claras para que los usuarios puedan aceptar o rechazar la recopilación de datos, así como ofrecer una manera sencilla de retirar su consentimiento si lo desean.

Responder a las solicitudes de los usuarios

Tanto el GDPR como la CCPA otorgan a los usuarios el derecho de acceder, modificar o eliminar sus datos. Aunque la plataforma de Fivvy no maneja información personal, las empresas deben proporcionar una forma para que los usuarios gestionen sus datos o soliciten la eliminación de los datos vinculados a su Device ID.

Monitorear los cambios en las regulaciones de privacidad

Las leyes de privacidad están en constante evolución. Es esencial que las empresas se mantengan actualizadas sobre nuevas regulaciones o enmiendas a las leyes existentes que puedan afectar sus prácticas de recopilación de datos. Fivvy proporciona actualizaciones periódicas sobre cualquier cambio que pueda impactar el uso de nuestra plataforma y los pasos que deben seguir las empresas para seguir cumpliendo con las normativas.

6 Conclusión

Al utilizar la plataforma de Fivvy, las empresas pueden garantizar el cumplimiento de las regulaciones de privacidad globales mientras aprovechan los potentes insights que proporcionamos a través de datos anónimos. Nuestro modelo de privacidad desde el diseño reduce la complejidad del cumplimiento normativo, y apoyamos activamente a nuestros clientes para mantener la conformidad con el GDPR, CCPA y las políticas de las tiendas de aplicaciones. Con Fivvy, las empresas pueden centrarse en la toma de decisiones basada en datos sin el riesgo de infringir la privacidad de los usuarios o las obligaciones regulatorias.

Seguridad de Datos e Infraestructura

En Fivvy, la seguridad de los datos es un aspecto fundamental de nuestra plataforma, y lo logramos aprovechando la infraestructura de Amazon Web Services (AWS). AWS ofrece medidas de seguridad líderes en la industria, garantizando que los datos recopilados a través de la plataforma de Fivvy estén protegidos en todas las etapas de su ciclo de vida. Al utilizar AWS, nos beneficiamos de una infraestructura robusta, escalable y conforme a las normativas, que respalda nuestro compromiso con la privacidad, la encriptación, el control de acceso y el cumplimiento regulatorio. Además, Fivvy emplea una estrategia de data lakehouse para gestionar y almacenar grandes volúmenes de datos de manera eficiente, asegurando flexibilidad y un manejo seguro de la información para múltiples casos de uso.

1 Encriptación de Datos: Garantizando la Seguridad de la Información en Todo Momento

Uno de los aspectos más críticos de la seguridad de los datos es la encriptación, que asegura que la información permanezca inaccesible para entidades no autorizadas, incluso si es interceptada o comprometida. AWS ofrece mecanismos de encriptación completos para proteger los datos tanto en su estado almacenado (en reposo) como durante su transmisión.

2 Encriptación en Reposo

Los datos recopilados por Fivvy se almacenan en AWS utilizando encriptación AES-256, un estándar de encriptación altamente seguro y ampliamente adoptado en la industria. AES-256 asegura que los datos estén protegidos mediante claves de encriptación de 256 bits, lo que hace que sea extremadamente difícil para cualquier entidad no autorizada descifrar o acceder a la información almacenada. La encriptación en reposo de AWS se aplica a todos los datos almacenados en servicios de AWS, como Amazon S3, Amazon RDS o Amazon DynamoDB.

3 Encriptación en Tránsito

Los datos están igualmente protegidos mientras se transmiten entre los clientes de Fivvy y la infraestructura de AWS, o entre diferentes servicios de AWS. AWS utiliza protocolos de Seguridad de la Capa de Transporte (TLS) para garantizar que los datos estén encriptados mientras viajan por la red, evitando posibles intercepciones o ataques de intermediarios. Esto significa que, ya sea que los datos se estén cargando, procesando o transfiriendo entre aplicaciones, siempre estarán encriptados y seguros.

4 Gestión de Claves

AWS proporciona herramientas como AWS Key Management Service (KMS) para gestionar de manera segura las claves de encriptación utilizadas para proteger los datos. KMS permite a Fivvy crear, controlar y gestionar claves de encriptación con controles de acceso detallados,

garantizando además que solo los procesos o el personal autorizado puedan descifrar los datos cuando sea necesario.

Certificaciones de Cumplimiento: Cumpliendo con Estándares Globales

Uno de los principales beneficios de usar AWS es su amplia gama de certificaciones de cumplimiento, las cuales ayudan a Fivvy a cumplir con los más altos estándares de seguridad y protección de datos. AWS está certificado bajo una amplia variedad de marcos de seguridad globales, garantizando que la infraestructura que utilizamos esté alineada con estrictos requisitos regulatorios.

ISO 27001

ISO 27001 es un estándar reconocido a nivel mundial para la gestión de la seguridad de la información. La certificación ISO 27001 de AWS garantiza que la plataforma ha implementado las mejores prácticas y controles para gestionar los riesgos de seguridad de la información. Esta certificación asegura que Fivvy opera en un entorno donde la seguridad de los datos se gestiona de manera estructurada y conforme a las normativas.

SOC 2

La certificación de cumplimiento SOC 2, especialmente importante para proveedores de SaaS como Fivvy, se centra en los principios de seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad. Al utilizar AWS, Fivvy garantiza que nuestra plataforma cumple con SOC 2, lo que significa que mantenemos controles rigurosos sobre cómo se gestiona, almacena y procesa la información.

HIPAA

Para las empresas que manejan datos relacionados con la salud, el cumplimiento de HIPAA es fundamental. AWS ofrece servicios compatibles con HIPAA, asegurando que cualquier dato de salud procesado a través de nuestra plataforma cumpla con los estándares de la Ley de Portabilidad y Responsabilidad de Seguros de Salud (Health Insurance Portability and Accountability Act). Aunque Fivvy se centra principalmente en datos anónimos, esta certificación brinda tranquilidad a los clientes de industrias reguladas, garantizando que sus datos se almacenan y procesan de manera segura.

Soporte para GDPR y CCPA

Aunque AWS en sí mismo no garantiza automáticamente el cumplimiento de GDPR o CCPA, proporciona las herramientas e infraestructura necesarias para que Fivvy mantenga el cumplimiento con estas regulaciones. AWS ofrece soporte para la localización de datos, encriptación y medidas de control de acceso que ayudan a cumplir con los requisitos de protección de datos y privacidad establecidos por GDPR y CCPA.

Gestión de Datos Flexible y Segura

Además de aprovechar las sólidas características de seguridad de AWS, Fivvy emplea una estrategia de data lakehouse para gestionar y procesar de manera eficiente las grandes cantidades de datos que recopilamos. Un data lakehouse combina las fortalezas de los data lakes y los data warehouses, lo que nos permite manejar datos estructurados y no estructurados en un entorno escalable, seguro y flexible.

Almacenamiento de Datos Unificado

Fivvy utiliza Amazon S3 de AWS para almacenar datos en bruto en su formato nativo, que funciona como nuestro data lake. Esto nos permite almacenar de manera segura y a gran escala enormes cantidades de datos no estructurados (como datos de uso de dispositivos y registros de interacción con aplicaciones). Para manejar datos estructurados y realizar consultas complejas en grandes conjuntos de datos, utilizamos Amazon Redshift, una solución de data warehouse potente. Este enfoque de lakehouse nos brinda la flexibilidad de almacenar todo tipo de datos mientras los mantenemos centralizados para un acceso y análisis más sencillo.

Procesamiento en Tiempo Real

Nuestra arquitectura de lakehouse nos permite procesar datos en tiempo real, extrayendo insights tanto de datos estructurados como no estructurados a medida que fluyen a través de nuestra plataforma. Esto es fundamental para ofrecer a nuestros clientes insights oportunos y accionables basados en el comportamiento de los usuarios en tiempo real.

Seguridad y Cumplimiento dentro del Data Lake

La seguridad y el cumplimiento siguen siendo prioridades principales incluso en nuestra estrategia de lakehouse de datos. AWS garantiza que todos los datos almacenados, ya sea en el data lake (Amazon S3) o en el data warehouse (Amazon Redshift), estén encriptados utilizando el estándar AES-256 para datos en reposo. Esto asegura que incluso los datos en bruto y no estructurados almacenados en nuestro data lake estén protegidos contra accesos no autorizados. Además, aplicamos encriptación en tránsito mediante protocolos TLS para asegurar el movimiento de datos entre nuestras capas de almacenamiento y motores de cómputo.

AWS's built-in access control mechanisms apply equally to both the data lake and the data warehouse environments. With AWS Lake Formation, Fivvy can establish granular permissions, ensuring that only authorized personnel can access specific datasets.

Aprendizaje Automático e Insights de Datos

Fivvy aplica técnicas avanzadas de Aprendizaje Automático (ML) a los datos que recopilamos de dispositivos móviles, transformando información en bruto en insights altamente accionables. Es importante destacar que estos insights se basan exclusivamente en el comportamiento anónimo de los dispositivos, garantizando el cumplimiento total de las leyes de privacidad y las regulaciones de la industria. A continuación, detallamos cómo utilizamos los datos a nivel de dispositivo y cómo nuestros modelos de ML generan insights valiosos sin acceder nunca a datos personales.

Comportamiento Anónimo del Dispositivo: Datos que Recopilamos

La recopilación de datos de Fivvy se centra exclusivamente en el comportamiento anónimo de los dispositivos, vinculado al ID del dispositivo. Los tipos de datos recopilados incluyen:

Uso de Aplicaciones

Rastreamos con qué frecuencia y durante cuánto tiempo los usuarios interactúan con aplicaciones específicas en sus dispositivos, proporcionando información sobre patrones de engagement. Esto incluye los tipos de aplicaciones utilizadas (por ejemplo, redes sociales, servicios de streaming, aplicaciones de la competencia), pero sin vincular estos comportamientos con información personal.

Información del Dispositivo

Recopilamos datos sobre el tipo de teléfono que se está utilizando (por ejemplo, iOS vs. Android, modelo de teléfono, versión del sistema operativo). Esto permite a nuestros clientes comprender mejor los tipos de dispositivos con los que interactúan sus usuarios, facilitando mejoras en el rendimiento de la aplicación y en la experiencia del usuario.

Tiempo de Uso

Fivvy registra la hora del día y la duración en que se utilizan aplicaciones específicas. Esta información es valiosa para comprender los hábitos de los usuarios y optimizar campañas de marketing o estrategias de interacción con los usuarios.

Toda esta información se recopila de forma anonimizada, ya que está vinculada únicamente al ID del dispositivo y no se realiza ningún intento por identificar al usuario detrás del dispositivo. No se recopilan datos personales, como nombres, direcciones o cuentas de correo electrónico, lo que garantiza que todos los insights generados permanezcan anónimos.

Generación de Insights Utilizando Machine Learning

Los modelos de Machine Learning de Fivvy utilizan los datos anonimizados mencionados anteriormente para crear insights accionables para nuestros clientes. Nuestros modelos están diseñados para identificar patrones, tendencias y comportamientos a partir de los datos, ayudando a las empresas a tomar decisiones informadas. Los aspectos clave del

funcionamiento de nuestros modelos de ML incluyen:

Análisis de comportamiento

Los modelos de aprendizaje automático analizan el comportamiento del dispositivo para comprender patrones de interacción con aplicaciones, tendencias de uso y cambios en las preferencias de los usuarios. Por ejemplo, nuestros clientes pueden determinar con qué aplicaciones de la competencia interactúan frecuentemente sus usuarios, lo que les permite ajustar sus estrategias de marketing en consecuencia.

Análisis predictivo

Nuestros modelos de aprendizaje automático generan conocimientos predictivos sobre comportamientos futuros, como predecir el abandono de usuarios o identificar qué usuarios tienen más probabilidades de interactuar con una aplicación de la competencia. Nuevamente, todas las predicciones se realizan basándose en el comportamiento anónimo del dispositivo, sin involucrar información personal.

Procesamiento de datos en tiempo real

La plataforma de Fivvy procesa los datos en tiempo real, asegurando que nuestros clientes reciban información actualizada sobre su base de usuarios. Esto les permite tomar decisiones oportunas sobre campañas de marketing, mejoras en la aplicación o lanzamientos de productos.

Arquitectura libre de sesgos para garantizar equidad y precisión en los insights generados. Como solo utilizamos datos anónimos a nivel de dispositivo, como patrones de uso de aplicaciones, tipos de dispositivos y horarios de uso, nuestros modelos están aislados de sesgos relacionados con datos demográficos personales, comportamientos o identidades. Esto asegura que factores discriminatorios—como raza, género o nivel socioeconómico—no puedan influir en el análisis o los resultados. Nuestro enfoque en datos no personales, basados en el comportamiento, garantiza que todos los insights sean imparciales, objetivos y se basen únicamente en las interacciones de los usuarios con las aplicaciones, asegurando equidad en todos los procesos de toma de decisiones derivados de nuestra plataforma.

Enfoque de Privacidad Primero: No se utiliza información personal

Es fundamental reiterar que en ningún momento del ciclo de recolección o procesamiento de datos se utiliza o accede a información personal. El modelo de privacidad desde el diseño de Fivvy garantiza que todos los insights se generen exclusivamente a partir de datos anónimos vinculados al ID del dispositivo. Los algoritmos de Machine Learning solo procesan datos completamente desvinculados de cualquier información personal identificable (PII, por sus siglas en inglés).

Sin acceso PII

Fivvy no accede ni puede acceder a detalles personales como nombres de usuarios, direcciones de correo electrónico o cualquier forma de información personal identificable (PII). Esta es una limitación tanto técnica como basada en políticas, que garantiza que operemos dentro de estrictos límites de privacidad.

Datos anónimos para obtener insights personalizados

Aunque los datos que utilizamos son anónimos, nuestros clientes aún pueden obtener insights personalizados correlacionando el ID del dispositivo con sus bases de datos internas de clientes. Esto les permite ofrecer ofertas o mensajes de marketing dirigidos a usuarios específicos sin infringir la privacidad de los mismos.

Comentarios finales

El enfoque de Fivvy para la recopilación y análisis de datos pone la privacidad, la seguridad y el cumplimiento normativo en el centro de cada operación, proporcionando a nuestros clientes una solución poderosa y consciente de la privacidad. Al enfocarnos exclusivamente en datos anónimos, como IDs de dispositivo, patrones de uso de aplicaciones y comportamientos específicos del dispositivo, garantizamos que nunca se recopile ni procese información personal identificable (PII). Este modelo de privacidad por diseño protege el anonimato de los usuarios al mismo tiempo que ofrece información altamente procesable a nuestros clientes.

Nuestro compromiso con la seguridad de los datos se refuerza mediante el uso de Amazon Web Services (AWS), una infraestructura en la nube líder que ofrece cifrado estándar de la industria tanto en reposo como en tránsito, controles de acceso robustos y una amplia gama de certificaciones de cumplimiento (ISO 27001, SOC 2, HIPAA). Esto garantiza que todos los datos procesados a través de nuestra plataforma permanezcan seguros y protegidos contra accesos no autorizados o brechas, brindando a nuestros clientes confianza en la integridad de sus datos.

Además, Fivvy opera en total alineación con las regulaciones globales de privacidad, incluyendo el Reglamento General de Protección de Datos (GDPR) y la Ley de Privacidad del Consumidor de California (CCPA). Apoyamos a nuestros clientes al garantizar que nuestros procesos de recopilación de datos, incluidos los mecanismos de consentimiento del usuario, cumplan con estas estrictas normativas. La recopilación de datos anónimos de nuestra plataforma y la estricta adhesión a los principios de minimización de datos permiten que las empresas permanezcan en cumplimiento con las leyes de privacidad, incluso a medida que las normativas evolucionan.

En resumen, Fivvy ofrece a las empresas lo mejor de ambos mundos: la capacidad de aprovechar conocimientos en tiempo real a nivel de dispositivo que impulsan el rendimiento y la toma de decisiones, sin comprometer la privacidad y seguridad de sus usuarios. Nuestra plataforma está diseñada para adaptarse a cualquier entorno normativo, permitiendo a las empresas enfocarse en el crecimiento mientras nosotros gestionamos las complejidades del anonimato, la seguridad y el cumplimiento. Ya sea garantizando la privacidad o navegando por regulaciones complejas, Fivvy está diseñada para proteger los datos de los usuarios mientras ofrece información poderosa, segura y procesable.