Product & Policy Updates for GDPR

12 APRIL 2018

OneSignal is committed to helping our clients be GDPR compliant when using our Web Push, Mobile Push, and E-mail products. Our business and legal team are working hand-in-hand with many of our existing clients to ensure compliance with EU law. Whether you are in the EU or not, we'd like to help make it easier for all of our partners to comply with GDPR.

While these specific suggestions and changes we're making will help you comply with GDPR, we also recommend that your consult with your legal counsel for compliance recommendations specific to your company.

Some of the major changes we're making include updating our legal terms and our push and email products to limit our access to and what data is stored from EU users. We've been working closely with our legal team to update our EULA and make these product updates before the May 25th deadline.

Specific product changes include:

1. Providing the option to not store end-user IP addresses, and by default, not storing the IP addresses of end-users from countries within the EU.
2. For all clients, beginning on May 21st, 2018, we will discontinue building data models with data nor will we monetize any EU user data with our business and analytics partners. For our Enterprise clients, we have introduced a Data Processor Agreement (DPA) which formally designates us as a Processor for all data.
3. Releasing updated versions of our SDKs to make it easier for our clients to prevent user data from being sent to OneSignal until a user explicitly consents,
4. Adding support to our API for the deletion of user data. Additionally, we are reducing our data retention period of deleted data to 72 hours.
5. Updating our user data exporting capabilities to make it easier to search for and export user data from OneSignal. This will help our clients meet individual user requests for restriction, erasure, and data portability.
6. Preparing a guide on how to use OneSignal for push notifications without sending us personal user data.

In addition to the product changes, we've taken steps internally to ensure that all data sent to OneSignal is stored securely. These steps include auditing the software we use for security vulnerabilities, ensuring we're using up-to-date versions, improving network security in out datacenter, and ensuring we maintain and follow security best practices internally to ensure that we prevent unauthorized access to our servers.

For clients who use OneSignal in their apps or websites and who have EU users or are based in the EU, you are responsible for ensuring that you have a valid legal basis (e.g., consent, legitimate interest) for the personal data that is being sent to OneSignal. We recommend working with your legal counsel for guidance on your specific responsibilities. We are happy to work alongside you and your legal team to ensure compliance while using our services.

If you have any questions or concerns about this topic, our team is happy to answer any questions you have. Please send your inquiries to support+gdpr@onesignal.com.