# AppsFlyer's data management

Transparency is a key value in AppsFlyer's security and privacy practices. As a global data processor, it is critical for our customers and partners to understand how AppsFlyer stores, manages, and encrypts data and for how long.

### Data locations

AppsFlyer utilizes two data centers, both located within the EU:
Dublin, Ireland (AWS)
St. Ghislain, Belgium (GCP)

### Data in the cloud

AppsFlyer's data is stored in a private account on a public cloud (AWS and GCP). These cloud services follow a multi-tenancy approach of logical segregation.

### Data monitoring

AppsFlyer monitors all access and attempts to access data, 24/7. Customers have full visibility into access history (as well as failed attempts) and data usage in their account via audit trail.

### Data encryption

Data processed by AppsFlyer is encrypted at rest using AES256bit, while data in transit is encrypted via TLS 1.2 (port 443).

### Data retention

End-user data is retained for up to 24 months. Customers can allow end-users to delete specific data using our API.

### Data compliance

AppsFlyer maintains a strict data protection program. AppsFlyer's data centers are in full compliance with GDPR and global privacy regulations.

## The industry's most comprehensive compliance program

Learn more at appsflyer.com/trust