AppsFlyer

Brazil's LGPD

Disclaimer

A word from our lawyers: Nothing stated here is legal advice. It is provided for your information and convenience. We strongly encourage that you work closely with legal and other professional advisors to determine exactly how the Brazilian General Data Protection Law applies to you.

AppsFlyer

What is the LGPD?

The LGPD, the Lei Geral de Proteção de Dados (General Data Protection Law), often referred to as the "Brazilian GDPR", is a privacy regulation in Brazil which came into effect August 2020 and the final step in enforcement was activated in August 2021.

Similar to Europe's GDPR, the intention of the LGPD is to harmonize and strengthen data privacy laws in Brazil, empower individuals, and to reshape the way organizations handling personal data approach data privacy.

Who does the LGPD apply to?

The LGPD has an extraterritorial scope applying to companies regardless of where they are headquartered or where the personal data is actually processed.

Specifically, the LGPD will apply to you if:

- You process personal data in Brazil;
- The personal data was collected in Brazil; or
- The purpose of the processing is to offer or provide goods or services to individuals located in Brazil.

Therefore, in practice, you should assume you are subject to the LGPD, regardless of where you are headquartered if the personal data processed relates to individuals located in Brazil or was collected from individuals located in Brazil at the time of collection.

What information does the LGPD apply to?

The LGPD defines personal data very broadly, essentially covering any data that, by itself or combined with other data, could identify a natural person or otherwise subject such a person to certain treatment.

Under what terms are companies allowed to collect and process Personal Data under the LGPD?

Similar to the GDPR, the LGPD requires entities to have a legal basis in order to collect and/or process personal data. These include:

1. consent;
2. as needed for execution of a contract or preliminary procedures related to a contract;
3. to comply with a legal obligations and judicial, administrative and arbitration procedures;
4. for the protection of the life or physical safety of the data subject or third party;
5. by public administrations as necessary for the execution of public policies;
6. for protection of health, in procedures carried out by health care/ sanitary professionals;
7. for the protection of credit;
8. for carrying out studies by research entities (provided where possible using anonymization);
9. for legitimate interests of the controller or third party.

What rights do individuals have under the LGPD?

With transparency as one of the LGPD's key principles, individuals have a general right to be informed of the processing in a clear, adequate, and ostensive manner. Data subjects will also have the following rights:

- access to the personal data processed;
- deletion of personal data where processing based on consent, was extensive or unnecessary;
- revocation of consent;
- portability;
- rectification;
- disclosure of subprocessors and other third parties with whom personal data is shared;
- information about consent choices and the consequences of refusing consent; and
- confirmation of the existence of processing;

In addition, data subjects may also request an explanation about any automated decision-making by the controller and that a natural person review decisions that were based on such automated decisions. Clear and adequate information about the criteria and procedures used for automated decision-making must be provided in response to such requests.

What are the consequences for non-compliance?

Consequences may include fines and penalties that reach up to 2% of a company's gross revenues in Brazil in the previous year, or 50 million Reais – (approximately US$10 million), whichever is greater, per violation.

Additionally companies may be compelled to temporarily or permanently suspend all processing activities for certain violations.

What this means for customers using AppsFlyer:

At AppsFlyer, privacy and security are always at the forefront. To ensure our customers have the tools and assurances they need to comply with the LGPD, AppsFlyer has taken timely action.

Similar to the GDPR, the LGPD separates between the data controller and the data processor.

- The data controller is the person or entity in charge of making decisions regarding the processing of personal data.
- The data processor is the person or entity that processes personal data in the name of the controller.

In the context of using the AppsFlyer services, the data controllers are the AppsFlyer customers and the data processor is AppsFlyer.

The AppsFlyer services are essentially an extension to the customer's technology stack (similar to a CRM). The personal data processed belongs to the customer. AppsFlyer will only process the personal data to provide the service as instructed by the customer under the terms of the agreement between the parties (and as further described in the **AppsFlyer Services Privacy Policy**.

As data controllers, AppsFlyer's customers will need to comply with all requirements of the LGPD that apply to them as data controllers. Controllers will need to, among other things:

- provide appropriate privacy notices to data subjects about their personal data processing
- ensure they have procedures in place to respond to data subject requests
- maintain appropriate records of their data processing (data mapping)
- ensure records of valid consents maintained when legal basis is consent
- appoint a data protection officer and publish his contact details
- implement an appropriate data security program and incident response plan for data breaches
- implement privacy by design principles
- comply with cross border transfer requirements

“Personal Data” under the LGPD and using AppsFlyer:

Even though AppsFlyer restricts customers from configuring the service to collect personal data such as names, contact information, addresses, financial information or any sensitive personal data, due to the very broad definition of “Personal Data” under the LGPD, it is likely that device identifiers such as Advertising ID’s (IDFA, GAID) or network data such as IP address is deemed personal data and thus the data collected when using AppsFlyer is subject to the LGPD requirements.

For more information on the data types processed when using AppsFlyer please visit the AppsFlyer Services Privacy Policy.

AppsFlyer supports deletion or access requests from individuals:

AppsFlyer has an infrastructure in place in support of global data subject requests, that enables customers to make data deletion and access requests through simple API calls utilizing its OpenGDPR framework. Customers will be able to utilize OpenGDPR to comply with any data subject access and deletion requests they receive under the LGPD, and allows for deletions within the prescribed 15-day window.

Cross-border transfer of personal data (outside of Brazil):

The LGPD permits international transfers provided there is a valid legal basis – for example, where prior valid consent was given. Additionally, transfers will be permitted to a country or organization that provides an adequate level of protection of personal data, or where there are guarantees of compliance to the LGPD principles through:

- specific contractual clauses for a given transfer;
- standard contractual clauses;
- global corporate rules; and
- valid seals of quality, certificates and codes of conduct.

Currently AppsFlyer processes its data at AWS and Google Cloud in the EU. In providing support and maintenance to AppsFlyer customers, data may also be accessible in other territories where AppsFlyer provides services, including, Israel.

Therefore, since AppsFlyer processes personal data outside of Brazil (primarily in the EU and Israel), customers need to ensure they receive valid consent from their end users.

Can customers 'opt-out' an end-user from measurement if they don't provide consent?

Yes, AppsFlyer provides its customers with **multiple options** to support whatever framework customers wish to implement (opt-in, opt-out, no postbacks, etc).

AppsFlyer's data processing commitments

AppsFlyer's Data Protection Addendum ("DPA") and commitments under the DPA cover personal data as defined under global regulations including the LGPD. The DPA is incorporated into the AppsFlyer terms of use by reference and therefore customers will not need to take any actions. Our DPA is available here and includes, among other things:

1. A definition of each party's status under the LGPD: AppsFlyer as a Data Processor and Customer as the Data Controller;
2. AppsFlyer's commitment to processing data per the instructions of its customers as provided under their agreements;
3. AppsFlyer's commitment to ensuring it has appropriate technical and organizational measures to protect customer's personal data;
4. AppsFlyer's commitment to supporting customers with their compliance requirements including those related to reporting, data breaches, privacy impact assessments and data subject rights; and
5. A list of the subprocessors utilized by AppsFlyer and the procedures for adding any new subprocessors.

For customers who have executed a previous version of the DPA or wish to have an executed copy of the DPA, you are welcome to download and execute the new version available at **https://www.appsflyer.com/gdpr/dpa.pdf** (which has been pre-signed by AppsFlyer) and to submit an executed copy to **privacy@appsflyer.com**. Regardless of whether you execute such modified version or not, be assured that AppsFlyer will process personal data subject to the LGPD pursuant to the terms set forth under the current DPA.