

Notice at Collection and Privacy Policy

Last Updated: December 2025

At Digital Turbine USA, Inc. (“DT,” “we,” “us,” or “our”), we make a concerted effort to ensure that we secure personal information and use it responsibly.

This notice at collection (the “**Notice at Collection**”) and Privacy Policy (the “**Policy**,” and collectively: the “**Notice**”) explain to you (“**User**” or “**you**”) our privacy practices for processing personal information related to you when you choose to install a mobile application on your device, and such installation is performed by our app installer (the “**Services**”). Our Services’ software will download your selected app directly to your device without going through the Google Play Store.

In this Notice, the term “**personal information**” refers to information that identifies an individual or relates to an identifiable individual and includes equivalent terms such as “**personal data**” or as otherwise defined under applicable data protection and privacy laws of the United States (“**US Privacy Laws**”) or under the GDPR, UK GDPR, and LGPD (collectively with the US Privacy Laws, “**Privacy Laws**”). The notice also explains certain rights that Users have under Privacy Laws and how they may exercise them.

The general part of this Policy applies to all Users of our Services. The **ANNEX** to this Policy includes supplemental terms regarding processing personal information under the GDPR, UK GDPR, and LGPD.

We operate the Services as a controller/business (within the meaning of Privacy Laws).

The summary below will give you a quick and clear view of our practices. The first six headings in the summary also serve as the Notice at Collection. Please, however, take the time to read our full Notice. If you disagree with its terms, please do not access or use our Services.

▪

Notice at Collection and A Summary of the Policy		
NOTICE AT COLLECTION	Categories of personal information Read More	When you engage with our Services, we collect and store the minimal information that is necessary to record an installation of mobile application on your device. We process only your Android Advertising ID (AAID) in pseudonyms form alongside non-personal information and signals related to your device.
	Categories of sensitive personal information Read More	The Services do not collect sensitive personal information (within the meaning of Privacy Laws.
	What do we do with personal information? Read More	The personal information related to you is processed to enable and measure the installation of mobile applications on your mobile device via our Services.
	Who do we disclose, share, or sell personal information with? Read More	We share your device Advertising ID with Mobile Measurement Platforms (MMPs) solely for attribution and invoicing purpose. We do not sell, or share personal information related to you with any third party for cross-context behavioral advertising. We may share personal information related to you when we change our corporate structure. We may share personal information related to you to obey court orders and other lawful requirements by authorities to disclose information.

	How long do we retain personal information? Read More	We retain personal information for up to thirty (30) days, and when necessary, for a longer period for legitimate and lawful purposes, such as disputes, compliance with applicable laws, and service development.
	Your choices and rights Read More	You have several opt-out options with respect to our processing of personal information related to you in connection with the Services. For example, you may opt-out of using the Services by opting out via the settings of the notification prompts you to opt-in to the Services, or via the Android standard setting. You also have privacy rights under applicable privacy laws, which you can contact us to exercise.
	Children Read More	We do not knowingly process, sell or share personal information related to children, as such term is defined under applicable privacy laws and regulations such as the Children Online Privacy Protection Act (COPPA).
	Exercising your choices and rights Read More	You can stop using the Services at any time, and thereafter, we will stop collecting personal information related to you. You may request to exercise the rights detailed under the “ <i>Your Choices and Rights</i> ” section by submitting your request to us by emailing: privacy@digitalturbine.com . You may also control what personal information we collect from your device by changing the permissions settings on your mobile device.
	Transfer of personal information outside your territory Read More	We store personal information related to you in the United States. Our service providers provide us with adequate security and confidentiality commitments.
	Aggregated and analytical information Read More	Aggregated data is not identifiable and, therefore, not personal information. We use it for legitimate business purposes and standard analytical tools.
	Information security Read More	We implement systems, applications, and procedures to secure personal information related to you, to minimize the risks of theft, damage, loss of information, or unauthorized access or use of information.
	Dispute resolution Read More	Contact us at: privacy@digitalturbine.com or write us for every request and complaint. We will make good-faith efforts to resolve any existing or potential dispute with you.
	Changes to this Notice Read More	We will update our Notice from time to time after giving proper notice.
	Contact us Read More	Please contact us at: privacy@digitalturbine.com for further information.

The Digital Turbine Privacy Policy

Categories of personal information

When you use our Services, we collect the following personal information about you:

- Your Android Advertising ID (ADID).
- Device information such as device type, language, country code, operating system, APK version, network connection and type, etc.

Accordingly, in the preceding 12 months, we have collected the following categories of personal information:

- Your Android Advertising ID.
- The mobile applications that were installed on your mobile device via the Services.

We obtain the categories of personal information related to you listed above from the following categories of sources:

- Directly and indirectly from you and your use of our Services and your mobile device.
- Third parties such as Google.

Categories of sensitive personal information

Our Services do not collect sensitive personal information (within the meaning of applicable privacy laws and regulations). We do not knowingly collect sensitive personal information and require you not to provide us with any such information. We do not process sensitive personal information to infer characteristics about you, and we do not sell or share sensitive personal information for cross-context behavioral advertising.

What do we do with personal information?

We use personal information related to you for the following purposes:

- To enable the measurement of mobile applications installed on your mobile device via the Services.
- To fix errors related to the Services and for operational and technical purposes in relation to us providing the Services.
- To protect the services, networks, and systems, including cybersecurity measures.
- To provide support, customer relations, and service operations.

We obey the law and expect you to do the same. If necessary, we will use personal information related to you to enforce our terms, policies, and legal agreements, to comply with court orders and warrants, and assist law enforcement agencies, to collect debts, prevent fraud, misappropriation, infringements, identity thefts and any other misuse of the Service, and to take any action in any legal dispute and proceeding.

We commit to only process personal information related to you for the purposes described in this policy.

Who do we disclose, share, or sell personal information with?

Personal information related to you is disclosed to certain members of our staff who receive appropriate information security and privacy training, external consultants, and our affiliates, who are all governed by this Policy.

We also disclose personal information related to you to our agents worldwide and to third-party service providers that process personal information about you on our behalf. Such agents and service providers will be contractually bound to keep personal information related to you confidential and appropriately secure.

A merger, acquisition, or any other structural change will require us to transfer personal information related to you to another entity as part of the structural change, provided that the receiving entity will comply with this Notice.

We may engage third parties to provide us with services such as analytics (for example, Google Analytics for Firebase), marketing automation, and user experience, and we may allow them to collect personal information on our Services for the purposes and via the means described in their respective privacy policies <https://policies.google.com/privacy>; <https://firebase.google.com/support/privacy>.

We share your device Advertising ID with Mobile Measurement Platforms (MMPs) solely for attribution and invoicing purposes.

The categories of personal information collected by these third parties in the preceding 12 months include identifiers, online activities, and inferences drawn from such activities.

We will also need to disclose personal information related to you in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

How long do we retain personal information?

We retain the identifiers associated with your mobile device for up to 30 days, after which we anonymize/de-identify them so they are no longer personal information related to you.

We will keep aggregated non-identifiable information without limitation, and to the extent reasonable, we will delete or de-identify potentially identifiable information when we no longer need to process the information.

We may retain your personal information for longer periods according to legal requirements under applicable law.

Children

We do not knowingly sell or share personal information related to children, as such term is defined under applicable Privacy Laws.

Your choices and rights

- **Access.** You have the right to request confirmation from us whether we are processing personal information about you and to access such information, including to request to know:
 - what personal information we have collected about you;
 - what personal information about you we have shared or sold, within the meaning of US Privacy Laws;
 - the categories of sources from which personal information about you is collected;
 - the business or commercial purpose for collecting, selling, or sharing personal information about you;
 - the categories of third parties to whom we disclose personal information; and,
 - the specific pieces of personal information we have collected about you.
- **Correction.** You have the right to request that we correct inaccurate personal information that we maintain about you.
- **Deletion.** Personal information related to you is retained by us for up to thirty (30) days. After the retention, we no longer store any personal information related to you on our systems.
 - As a reminder, Users can **opt out of using the Services** by opting out via the “Settings” of the notification that prompts them of app delivery or via the Android standard setting:
 - Step 1: Open the “Settings” app on your device.
 - Step 2: Select the “Apps” or “Apps & Notifications” option.
 - Step 3: You may need to select “See All Apps” to view all opened applications.
 - Step 4: Tap the application you wish to force close (in relation to our Services, it will be named “Ignite”).

- You can also **remove the mobile application installed** on your device via the Services by using the “Settings” app on your device, which will disable the Services on your device. To remove an installed app:
 - Go to the device Settings-->Apps or Application Manager.
 - Then tap the app you want to uninstall (you may need to swipe right or left to find the app).
 - Then tap ‘Uninstall’. Upon disabling the Services’ app, the Service will no longer be available to you, and we will cease processing any personal information related to you.
- To **delete the personal information** related to you that we have in our possession, you may either (a) reset your device’s advertising ID or (b) delete your device’s Advertising ID. Both actions are available from the Android Settings menu > Google > Ads. To turn off notifications on your device, follow these steps:
 - Long-press on the notification.
 - Tap "Turn off notifications."
 - Select the specific notification channels you wish to disable or choose the top option to turn off all notifications.
 - Tap "Save."

Please review Google's support page, which mirrors these directions and offers a few other methods for disabling notifications on your device: <https://support.google.com/android/answer/9079661?hl=en#zippy=%2Cturnnotifications-on-or-off-for-certain-apps>

- You also have the right to request that we delete personal information related to you that we have collected from you, subject to certain exceptions under applicable privacy laws and regulations. Accordingly, note that when we delete personal information related to you, it will be deleted from our active databases. Still, as set forth above, we will retain your personal information for legitimate business purposes.
- **Portability.** When exercising your right of access detailed above, you may also have the right to obtain the personal information in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the information to another entity without hindrance. You may only exercise this right up to two times per calendar year. Also note that when responding to your request, we will omit any information that would disclose our trade secrets, as permitted by applicable privacy laws and regulations. You may also have the right to obtain a representative summary of the personal information you previously provided.
- **Opt-out rights.** You can opt out of our Services at any time as described above.
- **Non-discrimination.** You have the right not to receive discriminatory treatment by us for exercising your privacy rights, detailed in this Notice.
- If you are a European Economic Area (EEA) resident, you might have additional rights under the General Data Protection Regulation (GDPR). Please read our Supplemental Terms for Processing Personal Data Under the GDPR in the **ANNEX** to this Policy.

Exercising your choices and rights

We will give you choices about how we use and share personal information related to you, and we will respect your choices.

We collect and receive personal information related to you that we need for the purposes described in this Notice. You can stop using the Services at any time; thereafter, we will stop collecting personal information related to you. However, as detailed above, we will store and continue to use or make available certain personal information related to you.

If you want us to delete personal information related to you or you wish to receive a copy of such personal information, email us at privacy@digitalturbine.com.

Only you or a person authorized to act on your behalf may make a request related to personal information related to you. Access requests can be made by you only twice within a 12-month period.

The verifiable consumer request must provide sufficient information to allow us to reasonably verify that you are the person about whom we collected personal information or an authorized representative and describe your request with sufficient detail to allow us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with the requested personal information if we cannot verify your identity or authority to make the request and confirm the personal information related to you. We will only use the personal information provided in your request to verify your identity or authority to make the request.

We will do our best to respond to your request within 45 days of its receipt or 30 days, as mandated by applicable privacy laws and regulations in your country or state of residence. If we require more time (up to an additional 45 days or 30 days, as mandated by applicable privacy laws and regulations in your country or state of residence), we will inform you of the reason and extension period in writing. At your option we will deliver our written response by mail or electronically.

Any disclosures we provide will only cover the 12-months period preceding receipt of your request. If applicable, our response will also explain the reasons we cannot comply with a request.

We do not charge a fee to process or respond to your request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will inform you of the reasons for such a decision and provide you with a cost estimate before completing your request.

We will not require that you create an account to exercise your rights under this Policy, and we will not increase the cost or decrease the availability of the Services based solely on the fact that you have chosen to exercise one of your rights under applicable privacy laws and regulations.

After receiving our reply, you can appeal against our decision by contacting us. We will review your appeal and provide you with our answer and our explanation of the reasons for our decision(s) within 60 days of receiving it. We will also provide you with a link (to the extent available) to submit a complaint with the relevant Attorney General under the applicable US State privacy laws.

You can avoid our collection of personal information related to you by avoiding opting into the Services from your mobile device.

Transfer of personal information outside your territory

We store and process information, including personal information, in the USA directly or using parties, processors, and sub-processors, such as cloud hosting service providers.

If you are a resident in a jurisdiction where the transfer of personal information related to you to another jurisdiction requires your consent, then you hereby provide us with your express and unambiguous consent to such transfer.

We ensure that our third-party service providers make adequate confidentiality and security commitments, and we will take all steps reasonably necessary to ensure that personal information related to you is treated securely and in accordance with this policy.

Aggregated and analytical information

We use anonymous, statistical, or aggregated information and will share it with our partners for legitimate business purposes. It has no effect on your privacy because there is no reasonable way to extract data from the aggregated information that we or others can associate specifically with you.

Information security

We are committed to ensuring the security of personal information. Our hosting services and we implement systems, applications, and procedures to secure personal information related to you and minimize the risks of theft, damage, loss of information, or unauthorized access or use of information. These measures provide sound industry-standard security.

However, please understand that no security system is impenetrable. Although we make efforts to protect your privacy, we cannot guarantee that the Services will be immune from any wrongdoings, malfunctions, unlawful interceptions or access, or other kinds of abuse and misuse.

Dispute resolution

We periodically assess our data processing and privacy practices to ensure compliance with this policy, update it when necessary, and verify that we display it properly and in an accessible manner. If you have any concerns about the way we process personal information related to you, you are welcome to contact our privacy team at privacy@digitalturbine.com or write to us.

We will look into your query and make good-faith efforts to resolve any existing or potential dispute with you.

Changes to this policy

We may update this policy from time to time. If the updates have minor, if any, consequences, they will take effect 14 days after we post a notice on the notification related to our Services. Substantial changes will be effective 30 days after we initially post the notice.

Until the new policy takes effect, if it materially reduces the protection of your privacy under the then-existing policy, you can choose not to opt in or opt-out from the Services; continuing to use the Services after the new policy takes effect means that you agree to the new policy. Note that if we need to adapt the policy to legal requirements, the new policy will become effective immediately or as required by law.

Contact Us

Don't hesitate to get in touch with us at privacy@digitalturbine.com.

Annex

Supplemental Terms for Processing Personal Data Under The GDPR

We at DT describe our privacy practices and Services in our Notice at Collection and Privacy Policy above (the “**General Policy**”). Please take the time to read it.

These terms supplement and are not a substitute for our General Policy. They add terms specifically related to our privacy practices associated with processing personal data under European data protection laws, namely the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”).

You should read both documents to understand the full scope of our privacy practices. If there are any overlapping provisions, these supplemental terms will prevail for our processing of personal data under the GDPR.

These terms use specifically defined terms under the GDPR, such as “personal data,” “processing,” “consent,” “data controller,” and “lawful grounds of processing.” If you are not familiar with these terms, please seek further guidance or contact our privacy team at privacy@digitalturbine.com with any questions that you may have about these terms.

Lawful Grounds of Processing

We process personal data related to you as a data controller when you use the Services based on the following lawful grounds:

- We provide you with our Services subject to the contracts that govern them (such as our Services' Terms of Use, which you opted into to use the Services). We will process personal data related to you, which is necessary to perform our contract with you (i.e., provide you with the Services, including technically enabling your safe usage and operation of such services).
- We will process personal data related to you to comply with our legal obligations and, where necessary, to protect your and others' vital interests.
- We may rely on our legitimate interests, which we have a good-faith belief that are not overridden by your fundamental rights and freedoms, for the following purposes:
 - To communicate with you, including for direct marketing purposes.
 - To protect our Ss and our networks and systems, including by using cyber security measures.
 - To provide support, customer relations, and Services operations.
 - To enhance and improve your and other users' experience with our Services.
 - To detect, contain, prevent, and handle cases of fraud and misuse of our Services.

Your Rights Under the GDPR

In addition to your applicable rights, as described under our General Policy, you have the following rights:

- You can request to access personal data that we keep about you and receive further information as described under the GDPR. If you find that the personal data related to you is not accurate, complete, or up to date, please provide us with the necessary information to correct it.
- You can request to delete or restrict access to personal data related to you. We will review your request and use our judgment, pursuant to the provisions of the applicable law, to make a decision about it.
- If we need to delete personal data related to you following your request, it will take some time until we completely delete residual copies of personal data related to you from our active servers and our backup systems.
- If you exercise one (or more) of the above-mentioned rights per the provisions of applicable law, you may request to be informed that third parties that hold personal data related to you under this Policy will act accordingly.
- You may ask to transfer personal data related to you per your right to data portability.
- You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.
- You have a right to lodge a complaint with a data protection supervisory authority regarding your habitual residence, your place of work, or the place of an alleged infringement of your rights under the GDPR.

Please note that when you send us a request to exercise your rights, we will need to reasonably authenticate your identity and location. We will ask you to provide us with credentials to make sure that you are who you claim to be and will ask you further questions to understand the nature and scope of your request.

If you have any concerns about how we process personal data related to you, you are welcome to contact our privacy team at privacy@digitalturbine.com. We will investigate your inquiry and make good-faith efforts to respond promptly. If we cannot help, you also have the right to make a complaint to the applicable data protection supervisory authority, as aforementioned.

Our DPO and Representatives

Our Data Protection Officer (DPO) can be reached at: privacy@digitalturbine.com.

Our EEA designated representative is: Rickert Rechtsanwaltsgesellschaft mbH and can be reached at: Colmantstraße 15, 53115 Bonn, Germany, art-27-rep-digitalturbine@rickert.law.

Transfer of Personal Data Outside the EEA

We store and process personal data in the U.S. From time to time, we will make operational decisions that will have an impact on the sites in which we maintain personal data.

We ensure that our third-party service providers provide us with adequate confidentiality, data protection, and security commitments in accordance with the GDPR. We will also take all steps reasonably necessary to ensure that personal data related to you is treated securely and in accordance with our General Policy and these supplemental terms.

We may transfer personal data related to you to other countries. Some of them are not recognized by the European Commission as providing adequate protection for personal data, and some of them, although recognized, require additional safeguards. We will use appropriate safeguards, in particular, by way of entering into the European Union (EU) Standard Contractual Clauses with the relevant recipients, rely on self-certifications, or comply with equivalent data transfer mechanisms. You can contact our privacy team at privacy@digitalturbine.com to receive more information related to our data transfer practices.

Please also see the section below titled “US Transfers” for additional information regarding our transfers of Personal Data outside the EEA to the US.

U.S. Transfers

We participate in the EU-US Data Privacy Framework (“**EU-US DPF**”), the UK Extension to the EU-US DPF (“**UK Extension**”), and the Swiss-US Data Privacy Framework (“**Swiss-US DPF**”), as set forth by the US Department of Commerce. You can review our Data Privacy Framework registration at: <https://www.dataprivacyframework.gov/list>.

We have certified to the US Department of Commerce that we adhere to the EU-US Data Privacy Framework Principles (“**EU-US DPF Principles**”) with regard to the processing of personal information received from the European Union in reliance on the EU-US DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-US DPF.

We have certified to the US Department of Commerce that we adhere to the Swiss-US Data Privacy Framework Principles (“**Swiss-US DPF Principles**”) with regard to the processing of personal information received from Switzerland in reliance on the Swiss-US DPF.

If there is any conflict between the terms in this notice or our policy with the EU-US DPF Principles (including the UK Extension) or the Swiss-US DPF Principles, the Principles will govern. To learn more about the Data Privacy Framework (“**DPF**”) program, visit the data privacy framework website [here](https://www.dataprivacyframework.gov).

In accordance with the EU-US DPF, we commit to resolve DPF Principles-related complaints about our collection and use of personal information related to you. If you have any inquiries or complaints about our handling of personal information received in reliance on the EU-US DPF, the UK Extension to the EU-US DPF, and the Swiss-US DPF (as applicable), please contact us at: privacy@digitalturbine.com. We will do our best to respond to your inquiry as soon as we can.

In accordance with the EU-US DPF, the UK Extension to the EU-US DPF, and the Swiss-US DPF, we commit to cooperate (respectively) with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC), as applicable, with regard to unresolved complaints concerning our handling of personal information received in reliance on the EU-US DPF, the UK Extension to the EU-US DPF, and the Swiss-US DPF.

You may also decide to invoke the arbitration option under the DPF, under certain conditions detailed [here](#). For additional details.

As explained under the section titled "Who do we disclose, share, or sell personal information with?" in our policy, we share personal information with third parties to perform services on our behalf.

When we share personal information received under the Data Privacy Framework with a third party, the third party's access to, and use and disclosure of such personal information, must also comply with our obligations under the Data Privacy Framework. We will remain liable under the Data Privacy Framework for any failure to do so by such a third party, unless we can demonstrate that we are not responsible for the event giving rise to the damage.

We are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Note that, as detailed above, we may be required to disclose personal information related to you in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Supplemental Terms for Processing Personal Data Under the LGPD

We at DT describe our privacy practices and our relevant services on our Notice at Collection and Privacy Policy (the "**General Policy**"). Please take the time to read our General Policy.

These terms supplement our General Policy. They add terms specifically related to our privacy practices associated with processing personal data under Brazilian data protection laws, namely the Brazilian General Data Privacy Law (Lei Geral de Proteção de Dados Pessoais). We will refer to them as the "**LGPD**").

You should read both documents to understand the full scope of our privacy practices. If there are any overlapping provisions, these supplemental terms will prevail, for our processing of personal data under the LGPD.

These terms use certain defined terms under the LGPD, such as "personal data", "processing", "consent", "data controller" and "lawful grounds of processing", as translated from the official version of the LGPD in Portuguese. If you are not familiar with these terms, please seek further guidance or contact our privacy team at: privacy@digitalturbine.com with any question that you may have about these terms.

Lawful Grounds of Processing

We process personal data related to you as a data controller when you use any of our ss based on the following lawful grounds:

- We provide you with our Services subject to the contracts that govern them (such as our Services Terms of Use or Terms and Conditions that you opted in to use such services). We will process personal data related to you, which is necessary to perform our contract with you.
- We will process personal data related to you to comply with our legal obligations and, where necessary, to protect your and others' vital interests.

- We may rely on our legitimate interests, which we have a good faith belief that are not overridden by your fundamental rights and freedoms, for the following purposes:
 - To communicate with you, including for direct marketing purposes.
 - To protect our Services and our networks and systems, including cyber security measures.
 - To provide support, customer relations, and service operations.
 - To enhance and improve your and other users' experience with our Services.
 - To detect, contain, prevent, and handle cases of fraud and misuse of our Services.

Your Rights Under the LGPD

In addition to your applicable rights, as described under our General Policy, you have the following rights concerning **personal data related to you**:

- Confirmation of the existence of the processing;
- Access to the personal data related to you (i.e., obtain a copy);
- Correction of incomplete, inaccurate, or out-of-date personal data related to you;
- Anonymization, blocking or deletion of unnecessary or excessive personal data related to you or personal data related to you processed in noncompliance with the provisions of the LGPD;
- Portability of the personal data related to you to another service or service provider by means of an express request and subject to commercial and industrial secrecy, pursuant to the regulation of the controlling agency;
- Deletion of personal data related to you processed with your consent, except in the situations provided under the LGPD;
- Information about public and private entities with which we shared personal data related to you;
- Information about the possibility of denying consent and the consequences of such denial;
- Revocation of your consent as provided under the LGPD.

Please note that when you send us a request to exercise your rights, we will need to reasonably authenticate your identity and location. We may ask you to provide us with your credentials to make sure that you are who you claim to be, and we may ask you further questions to understand the nature and scope of your request.

If you have any concerns about the way we process personal data related to you, you are welcome to contact our privacy team at privacy@digitalturbine.com. We will investigate your inquiry and make good-faith efforts to respond promptly. If we are unable to help, you also have the right to make a complaint to the applicable data protection supervisory authority, as aforementioned.

Our DPO

Our Data Protection Officer can be reached at privacy@digitalturbine.com.

Transfer of Personal Data Outside Brazil

Our Services are either provided via mobile application installed on your mobile device, or web-based service that is available on your mobile device. We store and process information within the U.S. From time to time, we will make operational decisions which will have an impact on the sites in which we maintain personal data.

We make sure that our third-party service providers provide us with adequate confidentiality, data protection and security commitments in accordance with the LGPD, and we will take all steps reasonably necessary to ensure that personal data related to you is treated securely and in accordance with our General Policy and these supplemental terms.

We will transfer personal data related to you to other countries. Some of them provide a degree of protection of personal data appropriate to the provisions the LGPD. In other cases, we will use appropriate safeguards by way of entering into standard data transfer agreements with the relevant recipients, or by relying on other applicable data transfer mechanisms. You can contact our privacy team at: privacy@digitalturbine.com to receive more information related to our data transfer practices.