Lightricks Ltd., including our subsidiaries and affiliates (collectively, “Lightricks”, “we”, “our” or “us”), puts great efforts in making sure that the personal data we process is stored securely and used properly, and that our data processing practices are accurately communicated to our users and prospective users.

Lightricks is a pioneer in innovative technology that bridges the gap between imagination and creation. Lightricks’ photo and video editing tools offer endless possibilities and inspiration, providing individuals, content creators, or influencers the ability to monetize their work and offer brands opportunities to scale their content through tailored creator partnerships. Lightricks is a global company, offering these services, apps and technology worldwide.

This Privacy Policy (“Policy” or “Privacy Policy”) describes how we collect, store, use and disclose information while using any of the services, technologies and apps detailed herein. We tried to detail these processes in a simple and friendly manner, however, as Lightricks offers various mobile and web-apps (each an “App”), features and feeds (“Lightricks Feed”), and an online marketplace (“Popular Pays Marketplace”) connecting brands and agencies (“Brand(s)”) and individuals, content creators, influencers (“Creator(s)”), all of which process your information differently, we encourage you to read carefully and reach out to us if you have any further questions.

This Policy is applicable to (collectively and separately, referred to as "you" or "your"): (i) prospects and visitors browsing our websites, landing pages, engaging with ads and campaigns promoting our services, blogs or other web-forms (“Prospect” or “Visitor”); (ii) users installing and using our Apps; (iii) Brands and Creators using the Popular Pays Marketplace; and (iv) any individuals using our services.

You are not required, at any time, to provide us with personal data or personal information.

POLICY TOPICS:
1. UPDATES AND AMENDMENTS ........................................................................................................... 2
2. CONTACT INFORMATION AND ROLES ................................................................................................. 2
3. TYPE OF DATA SETS PROCESSED ........................................................................................................... 3
4. PURPOSE, LAWFUL BASIS, AND PROCESSING OPERATIONS ......................................................... 3
    TABLE A: APPS ......................................................................................................................................... 3
    TABLE B: AI MACHINE LEARNING AND INTERNAL DEVELOPMENT .................................................. 8
    TABLE C: POPULAR PAYS MARKETPLACE ............................................................................................. 9
    TABLE D: PROSPECTS AND INDIVIDUALS INTERACTION WITH OUR WEBSITE, ADS OR DIGITAL ASSETS 12
5. HOW WE COLLECT YOUR INFORMATION ............................................................................................... 14
6. COOKIES AND SIMILAR TECHNOLOGIES ............................................................................................ 14
7. DATA SHARING – CATEGORIES OF RECIPIENTS WE SHARE PERSONAL DATA WITH ......................... 15
8. USER RIGHTS ............................................................................................................................................ 17
9. DATA RETENTION .................................................................................................................................... 17
10. SECURITY MEASURES .............................................................................................................................. 17
11. INTERNATIONAL DATA TRANSFER

12. ELIGIBILITY AND CHILDREN PRIVACY

13. SPECIFICATIONS
   i. Additional Notice to California Residents
   ii. Additional Notice to Colorado Residents
   iii. Additional Notice to Virginia Residents
   iv. Additional Notice to Connecticut Residents
   v. Additional Notice to Utah Residents (Effective January 2024)
   vi. Additional Notice to Nevada Residents
   vii. Additional Notice to Brazil Residents

1. UPDATES AND AMENDMENTS

We may update and amend this Policy from time to time, at our sole discretion. The most recent version of the Policy will always be accessible from the website or Apps. The updated date of the Policy will be reflected in the “Last Modified” heading. In case of a material change, or if required by law, we will provide notice reflecting these changes. Any amendments to the Policy will become effective within 30 days after we publish the modified Policy. We recommend you review this Policy periodically to ensure that you understand our most updated privacy practices.

2. CONTACT INFORMATION AND ROLES

Lightricks Ltd. is incorporated under the laws of the state of Israel and, unless otherwise explicitly mentioned in the table below, is the Controller of the Personal Data (as such terms are defined under the General Data Protection Regulations “GDPR” or equivalent privacy legislation).

For any questions, inquiries or concerns related to this Privacy Policy or the processing of your Personal Data, you may contact us as follows:

DPO Contact Information: dpo@lightricks.com

By Mail:
Lightricks Ltd.
Professor Racah St, Building 5.4,
Jerusalem, Israel, 9190401

Representative for data subjects in the EU and UK Contact Information:

We have appointed representatives in Germany and in the UK for data protection matters concerning EU or UK data subjects.

- Inquiries regarding our EU privacy practices may be sent to our Data Protection Representative (“DPR”) as follow:
DPR Contact Information: dpr@lightricks.com

By Mail:
Lightricks GmbH,
c/o Mazars Tax GmbH, Theodor Stern Kai 1, 60596 Frankfurt am Main, Germany.

- Inquiries regarding our UK privacy practices may be sent to our UK DPR as follow:

UK-DPR Contact Information: uk-dpr@lightricks.com

By Mail:
Lightricks (UK),
ICO Registration number: ZB253341

3. TYPE OF DATA SETS PROCESSED

During your use or interaction with the services, we collect aggregated, non-personal, non-identifiable information ("Non-Personal Data"). Non-Personal Data collected includes aggregated usage information, anonymized information, and technical information, such as: type of browser or device, language preference, time and date stamp, etc.

We further collect information that identifies an individual or may, with reasonable effort, be used to identify an individual ("Personal Data"). The types of Personal Data that we collect as well as the purpose for processing such data are specified in the table below. For the avoidance of doubt, any Non-Personal Data connected or linked to any Personal Data shall be deemed Personal Data as long as such connection or linkage exists.

We may process demographic data and certain profiling criteria, which is inferred from the data sets listed below, by means of example, from your pictures we may determine your gender and age.

4. PURPOSE, LAWFUL BASIS, AND PROCESSING OPERATIONS

We have detailed below, for each asset and services, the Personal Data processed, the purpose and operation and the lawful basis for such processing. There are four tables below, Table A details the Personal Data processed while using our Apps, Table B details the Personal Data used for development, AI machine learning, or otherwise used for internal purposes, Table C details the Personal Data processed when using Popular Pays Marketplace and Table D details the Personal Data processed when you interact with our website, ads, or otherwise.

<table>
<thead>
<tr>
<th>TABLE A: APPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA SET</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- **TABLE A: APPS**

<table>
<thead>
<tr>
<th>DATA SET</th>
<th>PURPOSE AND OPERATIONS</th>
<th>LAWFUL BASIS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Account Data:

After you install the App, you will log in and create your account (for iOS users, creating an account is optional).

You may choose to login using your Apple, Facebook or Google account or otherwise by entering your email address and choosing a password.

If you login through Facebook, Google or Apple, we will receive information connected to such account (depending on the privacy settings you chose) such as your name, profile picture, friends list, demographic data, and location.

We use the Account Data to create an account to authenticate the identity of you. If you use several Apps and you have signed in, we will be able to identify you across those various Apps and share the information processed in each of the Apps. We will further send you invoices, materials and content, including marketing materials, through the email address you provided during your registration (“Direct Marketing”).

Processing of the Account Data necessary for the performance of a contract.

Processing for Direct Marketing is subject to our legitimate interest, you may opt-out at any time by unsubscribing. Note, even if you unsubscribe certain operational emails will still be sent.

### Online Identifiers and Usage Data:

When you use the Apps, we, or our third-party partners, identify you through Online Identifiers. “Online Identifiers” are unique identifiers, including IDFA or AAID, IP address, device ID, cookie ID, agent, etc.

We further process, directly or indirectly through our third-party partners, usage data, which may or may not be associated with the Online Identifiers. When associated with an Online Identifier it will be treated as Personal Data, otherwise, if the usage data is aggregated, anonymized or de-identified, it will not be considered as Personal Data.

The usage data includes information regarding your interaction with the App, features used, duration of use, click stream data, errors that occurred, as well as your interaction with the Online Identifiers and Usage Data are used for analytics and operational purposes, correcting errors and bugs, adjust language preference, if applicable, to enable you to use the app and to provide you with its functionalities.

Some of the Apps further display interest-based ads or other marketing and promotions which are based on the Usage Data.

When the processing is for marketing or tracking, we will process the Personal Data solely based on consent.

When the processing of Personal Data is for operations and providing the App functionalities, the lawful basis would be contract necessity.

Last, the Personal Data maybe processed subject to our legitimate interest of understanding how our services are used, correcting errors and enhancing experience, including by personalizing offers and promotions.
content or ads displayed, records of advertising and content displayed on pages or App screens displayed to you, and any interaction you may have had with such content or advertising (collectively “Usage Data”).

<table>
<thead>
<tr>
<th>Images, Photos and Videos:</th>
</tr>
</thead>
</table>
| To enable the services, you will either provide us access to your photo gallery or upload photos from your gallery. Images, photos and videos are processed on your device to determine the estimated location of parts of faces (such as the eyes, nose or mouth) and points on the face and eyes, which are applied to a generic model of a face that is used to help you edit images and videos in real time (“Face Data”).

We also collect demographic data processed on iOS devices such as age and gender from your images, photos, videos.

When photos and images are used for creating artwork or adding effects to your creations, the selected image is uploaded to the Lightricks Cloud. No data is processed by these effects or is used to identify you, and no data is stored on the Lightricks Cloud except for the original image and the output image, which are deleted within 30-days unless you request otherwise.

<table>
<thead>
<tr>
<th>AI Tools and Avatars:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain apps include artificial intelligence (“AI”) technology for editing images, photos and videos, for creating personalized magical avatars (“Avatars”), motions and effects, art styles,</td>
</tr>
</tbody>
</table>

We use the data uploaded to the Lightricks Cloud, meaning the Input and the Output, for the purpose of providing the Services and generating the Output.

| |
| We process the data to enable the use of the features available within the Apps, including the ability to edit your images, videos and media. We will process the demographic data to market personalized offers by Lightricks. We do not use your actual photos, videos or Face Data for marketing purposes and this information is not shared with any third parties. Face Data is processed on your device. We do not collect or store Face Data on our servers or share it with third parties. |

| |
| We process the images, video and photos, including the Face Data for the purpose of providing the services and complying with our contractual obligations to you. If you choose to store projects that use Face Data, the data will be stored on your device until you delete the project, the project is deleted automatically due to storage limits, or you delete the App. If you granted access to your photo gallery, you can revoke the permission at any time. |

To create the Avatars, we process 10-25 images as Inputs for the purpose of providing the Services and comply with our contractual obligations to you. Currently we are using the neural network model Stable Diffusion that allows
For this, we will process the original images and videos uploaded ("Inputs") on the Lightricks Cloud. Our AI technology uses face detection to determine the posture, location and other non-identifying characteristics of faces that appear in frame, and may process non-user Personal Data as further described in the section below.

The Outputs are usually stored on your device and we do not have access or control over them, however, your purchased Avatars are stored on the Lightricks Cloud so that they remain accessible to you through the App at any time and from any device until you decide to delete them.

<table>
<thead>
<tr>
<th>Non-user Personal Data:</th>
<th>We process the photo solely for the purpose of providing the Services, we will not have any other use of the original photo. We will process your friend contact details only for the purpose of sending them an invite to use the Services, we will not use this data for any other purpose.</th>
<th>Legitimate interest in providing the Services to our User.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where we are able to determine that you have shared non-user Personal Data with us, such as the images or videos that you submit in connection with our “couples’ avatars” feature, we will use the images or videos to generate the avatar, or other Output and delete the Inputs permanently from the Lightricks Cloud. In addition, you may invite friends to use our Apps. By doing that you will be requested to share the contact details of your friend(s) (such as email address or phone number).</td>
<td>We process such information to provide the support services and fulfill the contractual obligations.</td>
<td></td>
</tr>
<tr>
<td><strong>Survey and Feedback:</strong></td>
<td>We use this information to improve, revise and enhance our Service, as well as optimize and customize the Services.</td>
<td>We process such information subject to your consent. You may withdraw your consent at any time by contacting us through the contact information provided herein.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Purchase Details:</strong></td>
<td>We use this information to process your payments.</td>
<td>Performance of our contract with you.</td>
</tr>
<tr>
<td>Certain features and Services are subject to payment, either in-app or subscription payments. Payments are made through in-app purchase (“IAP”) by third party payment services; however, we process the commercial transaction data such as, records of purchases and prices; shipping details (if applicable); address, contact telephone number and email address.</td>
<td>We may use third parties’ services and platforms to process the Payment Data, such as Adyen and Paypal, or through IAP in which Google Play or Apple Store would govern such payments. Consequently, any transactions processed by the third parties’ platforms will be governed by its own privacy policy and terms, which we recommend that you review.</td>
<td></td>
</tr>
<tr>
<td><strong>Social Media:</strong></td>
<td>We use the Feed Data to provide you with the Lightricks Feed Services and to enable your interaction with third party social media.</td>
<td>We process Feed Data for the performance of a contract with you. Note, information you choose to make public, may not be able to be deleted even if you delete the App and Account.</td>
</tr>
<tr>
<td>When you use Lightricks feed, or share your creations on social media, we will process Personal Data which you make available, such as profile photos, name, email address, social media accounts, reactions to feed posts (“Feed Data”).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Permissions:</strong></td>
<td>We will use these permissions to process the information needed to provide the Service or enhance the Service.</td>
<td>To access these App Permissions, you will need to actively and explicitly enable them through an in-app permission or the mobile settings, you can disable the App Permissions at any time, however note, depending on the App Permission you</td>
</tr>
<tr>
<td>Depending on the App used or the features you wish to enjoy, you will be asked to grant us access permissions such as: access to photo gallery, enable tracking tools, push notification, access to your social accounts, etc. (“App Permissions”).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For more information on the SDKs integrated on our Apps, please see below:

We use third-party analytics service providers such as Google Analytics, Google’s Crashlytics and Firebase services, and Facebook. We may disclose your information to these analytics providers to help us learn more about how you and others use our services:

- AppsFlyer SDK
- Nimble SDK
- AppLovin SDK
- Facebook iOS SDK
- Firebase iOS SDK
- Google signing iOS SDK
- Survey-Monkey iOS SDK
- TikTok SDK
- Braze SDK
- Full Story SDK
- Pendo.io

We will disclose the information to third party analytic providers for marketing and tracking purposes, analytics and operational purposes, correcting errors and bugs, adjust language preference, if applicable, to enable you to use the app and to provide you with its functionalities.

When the processing is for marketing or tracking, we will process the Personal Data solely based on consent. Otherwise, we will process these SDKs subject to our legitimate interest.

### TABLE B: AI MACHINE LEARNING AND INTERNAL DEVELOPMENT

<table>
<thead>
<tr>
<th>DATA SET</th>
<th>PURPOSE AND OPERATIONS</th>
<th>LAWFUL BASIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Usage Data; 2) Inputs, including the posture, location and other non-identifying characteristics of faces detected in Inputs by our AI technology (but not including Face Data, defined above).</td>
<td>We will use the data to enrich the content and improve the features available within the Services. We will use this information to personalize the service offered to you, tailor offers to your interest and offering additional Lightricks products, apps or services which we believe you will enjoy.</td>
<td>The machine learning and data labeling is processed subject to our legitimate interest to improve our Services and technology. We ensure that identifying information, such as device identifiers or Online Identifiers, is not associated with the information used for learning and training, including the Input, meaning the Input</td>
</tr>
</tbody>
</table>
To improve the AI technology and to offer better Services, we use parts of the Input in an **anonymized** manner, to train the algorithm and create models (such as diffusion models, GAN, and others). The Input cannot be linked to you, identified with you, or used to identify. We will not use the Input in whole but rather we will process certain copies extracted from the Input.

We will not be able to, and we do not aim to, authenticate or uniquely identify you, or any other person, using these models.

In addition, we automatically label certain images detected in your Input such as “dog”, “cat”, and male or female to improve the performance of the AI features, such as text-to-image and Avatar creation and for purposes of labeling data for use in machine learning. Note that labeled data is not tied to any identified individual.

Except as detailed above, models used for training and learning and are deleted within 180 days.

Please note that we do our best to moderate the setting of the AI model to not include any inappropriate or harmful content, however, it is your sole responsibility to upload images, videos, and other content that is not unlawful, libelous, defamatory, obscene, pornographic, indecent, lewd, suggestive, harassing, threatening, invasive of privacy or publicity rights, abusive, inflammatory, fraudulent, or can be otherwise interpreted as harmful content. Please contact us at dpo@lightricks.com if you find any content to be offensive. The use of the AI technologies is subject to the AI Terms as well, available at: https://static.lightricks.com/legal/ai-terms-of-use.pdf#page18.

**TABLE C: POPULAR PAYS MARKETPLACE**

<table>
<thead>
<tr>
<th>DATA SET</th>
<th>PURPOSE AND OPERATIONS</th>
<th>LAWFUL BASIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration:</td>
<td>We use this information to create an account, provide</td>
<td>Processing is necessary for the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>performance of a contract.</td>
</tr>
</tbody>
</table>
When the Brans signs up on Popular Pays Marketplace it shall fill in the contact information of the authorized users (name, phone number, email address, website, etc.).

Following registration and creation of the Brand Account, the Brand will have access to the dashboard which will include further data regarding its campaigns, statistics and analysis regarding its campaigns, user engagement, etc.

**Creator Accounts:**
A Creator will need to create a portfolio which will include full name, email address, age, gender, location, shipping address, demographic data, payment information (which will include your bank account details or Apple-Pay/ Google-Pay account), your profession or specializations (e.g., lifestyle, fashion, beauty, financing planning), language preferences, etc.

Any such information you make available through the portfolio is deemed “**Portfolio Data**”.

In addition, in order to participate in campaigns, the Creator will need to upload its creations to the portfolio, integrate its social media accounts through which Brands will be able to review the Creator’s work, bio and the account management, enable your interaction with the Creators, perform the marketing campaigns, provide support and any requested Services.

The campaign insights are provided in an aggregated analytic manner.

We use the Portfolio Data to create the portfolio, make it available for Brands to review, enable your interaction with the Brands, provide account management, provide support and any requested Services.

We further will use the content uploaded and the Portfolio Data to create aggregated insights on your audience and content (e.g., gender, age range, geo location, etc.).

Portfolio Data is necessary for the performance of our contract obligations in providing the services.

The insights are processed subject to our legitimate interest.

The creations you upload may also include Personal Data, however, we are the **Processor** (as such terms is defined under the GDPR) of such Personal Data, hosting the creations on your behalf.
type of followers the Creator interacts with.

<table>
<thead>
<tr>
<th><strong>Usage Data:</strong></th>
<th>We use this information solely for the purpose of improving the Services, fixing bugs and errors.</th>
<th>Processing is necessary for the performance of a contract.</th>
</tr>
</thead>
<tbody>
<tr>
<td>We collect information on how, when and where you use the service, access the Account, and actions conducted on the Popular Pays Marketplace.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Customer Support:</strong></th>
<th>We will use the contact information to provide the customer support needed. We will retain such correspondence for as long as needed, and to evidence the support was provided.</th>
<th>We process such information to provide the support services and fulfill the contractual obligations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you contact us for customer support, we will process your contact information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Direct Marketing:</strong></th>
<th>We will use this information to keep you updated with offers and content and for operations (invoices, offers, etc.).</th>
<th>We process such information subject to our legitimate interest. You can opt-out at any time through the “unsubscribe” link within the email at any time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>We will send you service communications and marketing promotions, such as new features, additional offerings, special opportunities or any other information we think you will find valuable.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Campaigns:</strong></th>
<th>We use such Insights for targeting campaigns on behalf of the Brand, as part of the services provided through the Marketplace.</th>
<th>We process this on behalf of the Brand as a Processor (as such terms is defined under the GDPR) and subject to the Brand’s instructions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>As a Brand, we provide services that enable you to deliver relevant content to end users, by targeting specific audience.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The targeted campaign will be directed to potential customers who appear to have the same or similar interests as the Brand’s existing customers, based on the segments we collect and analyze (&quot;Insights&quot;).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Booking a Demo:</strong></th>
<th>We will use this to provide you with the information or services that you have requested.</th>
<th>We process such information subject to our legitimate interest.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the event you choose to book a free demo, you will be requested to provide us with</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
your full name, phone number, and company email address.

**Purchase Details:**
Certain features and Services are subject to payment, either IAP or subscription payments by third party payment services; however, we process the commercial transaction data such as, records of purchases and prices; shipping details (if applicable); address, contact telephone number and email address.

We use this information to process your payments.

We may use third parties’ services and platforms to process the Payment Data, such as Adyen, Stripe, Braintre, and Paypal, or through IAP in which Google Play or Apple Store would govern such payments. Consequently, any transactions are processed by the third parties’ platforms will be governed by its own privacy policy and terms, which we recommend that you review.

<table>
<thead>
<tr>
<th>DATA SET</th>
<th>PURPOSE AND OPERATIONS</th>
<th>LAWFUL BASIS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online Identifiers and Usage Data:</strong> When you interact with our website, we, directly or indirectly collect Online Identifiers and Usage Data (i.e., access time and date, movement within the website, click stream, duration, referred URLs, content viewed, etc.). We process this information to improve the website, identify errors and bugs as well as for statistic, analytic and marketing purposes.</td>
<td>The Personal Data collected for operating the website, through first party cookies are based on our legitimate interest of enable the operation of the website and services. Depending on your jurisdiction, third-party cookies will be able to process Personal Data solely if you provided consent through the cookie notice and the consent management tool that is used on the website. You may withdraw consent at any time by using the cookie preference settings.</td>
<td>Subject to your consent through in-app permission or cookie banner, as applicable.</td>
</tr>
<tr>
<td><strong>Advertising:</strong> When we market the services, we use third party providers or tools to manage these ad campaigns. Through these tools, we collect information such as the individuals’ journey, To perform, facilitate and optimize our marketing campaigns, ad management and sales operations, and to manage and deliver advertisements for our products and services more</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
when they clicked our ad and if they installed, subscribed or engaged with such campaign or app. effectively, including on other websites and applications.

**Contact Information:**

If you voluntarily contact us through chat, email or other means, or if you fill in a survey, or provide feedback, you will be required to provide us with certain information such as your name, email address, and any additional information you decide to share with us.

If you are contacting us on behalf of another person, we value your assistance and care for others, please note that it is your responsibility to make sure that any person whose Personal Data you provide is aware of the principles of this statement and agrees that you will provide Personal Data to us on this basis.

We process the information to respond to your inquiry. We may also process the correspondence information in order to improve our sales services or customer support.

We process the information subject to our legitimate interest in order to respond to your inquiry. We may keep such correspondence if we are legally required to.

**Call Records:**

When contacting our Prospect, we might record the calls ("Call Records").

We use such Call Records in order to manage, measure and improve our sales efforts and enhance our Services.

We process Call Records subject to your consent which will be obtained at the beginning of our conversation.

**Newsletter Registration:**

In the event you sign up to receive our newsletter, blog updates or other marketing materials, you will be requested to provide your contact details, such as your email address.

We will use your email in order to send you our newsletter and other marketing materials.

We process such contact information subject to your consent. You may withdraw consent at any time through the “unsubscribe” link within the email or by contacting us directly.

Please note that the actual processing operation per each purpose of use and lawful basis detailed in the table above may differ. Such processing operation usually includes a set of operations made by automated means, such as collection, storage, use, disclosure by transmission, erasure, or destruction. The transfer
of personal data to third-party countries, as further detailed below under International Data Transfer Section, is based on the same lawful basis as stipulated in the table above.

In addition, we may use certain Personal Data to prevent potentially prohibited or illegal activities, fraud, misappropriation, infringements, identity thefts, and any other misuse of the Services and to enforce the Terms, as well as to protect the security or integrity of our databases and the Services, and to take precautions against legal liability. Such processing is based on our legitimate interests.

We may collect different categories of Personal Data and Non-Personal Data from you, depending on the nature of your interaction with the Services provided through the website, Apps, Web-Services and the Popular Pays Marketplace, as detailed above. If we combine Personal Data with Non-Personal Data, the combined information will be treated as Personal Data for as long as it remains combined.

5. HOW WE COLLECT YOUR INFORMATION

Depending on the nature of your interaction with us, we may collect the above detailed information from you, as follows:

- Automatically, when you visit our website or interact with our services, including through the use of Cookies (as detailed below) and similar tracking technologies.
- When you voluntarily choose to provide us with information, such as when you contact us or request a demo, all as detailed in this Policy.
- By our third parties service providers which collect personal data on our behalf, such as analytics service providers.

6. COOKIES AND SIMILAR TECHNOLOGIES

We may use cookies, tracking pixels (also known as clear GIFs and web beacons), third party software development kits (SDKs) as detailed in Table A above, and other technologies in order to maintain, provide, and improve our website, online platform and its services or our Apps. **We use Cookies for various purposes:**

- **Preferences:** this type of cookie helps us to secure and maintain our services, and remembers your preferences so you don’t have to re-set them each time you visit.
- **Statistics Cookies:** these tools are used for analytic purposes, to better understand the use of the services, Apps and websites.
- **Registration Cookies:** When you register and sign in, we generate cookies that let us know whether you are signed in or not.
- **Marketing Cookies:** These cookies allow us to know whether or not you’ve seen an ad or a type of ad, how you interacted with such an ad, and how long it has been since you’ve seen it. We also use cookies to help us with targeted advertising. We may partner with ad networks and other ad serving providers that serve ads on behalf of us and others on non-affiliated platforms. Some of those ads may be personalized, meaning that they are intended to be relevant to you based on information ad networks and ad serving providers collect about your use of our website and other sites or apps over time, including information about relationships among different browsers and devices. This type of advertising is known as interest-based advertising.
7. DATA SHARING – CATEGORIES OF RECIPIENTS WE SHARE PERSONAL DATA WITH

We share your data with third parties, including our partners or service providers that help us provide our Services. You can find here information about the categories of such third-party recipients.

<table>
<thead>
<tr>
<th>CATEGORY OF RECIPIENT</th>
<th>DATA THAT MAY BE SHARED</th>
<th>PURPOSE OF SHARING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essential Service Providers, which process data on our behalf, for the purpose of providing the services, securing and improving the services.</td>
<td>All data except for data which is stored locally on your device.</td>
<td>We may disclose Personal Data to our trusted service providers that provide technology or platforms that are essential for providing the Services (“Essential Service Providers”). Such Essential Service Providers include hosting, and server co-location services, communications and content delivery networks (CDNs), internet service providers, operating systems and platforms, data and cyber security services, fraud detection services, billing and payment processing services, shipping and handling services, session or activity recording services, support and customer relation management systems. Essential Service Providers have access, or process on our behalf. The Essential Service Providers are prohibited from using your personal information for any purposes other than providing us with requested services.</td>
</tr>
<tr>
<td>Marketing Service Providers</td>
<td>Behavior data, Usage Data, Online Identifiers, Account Data, and profiling data.</td>
<td>Our marketing service providers, that either process on our behalf certain data which we use to target you and offer you our Services, or they provide us with tools to do so (“Marketing Service Providers”).</td>
</tr>
<tr>
<td>Consultants</td>
<td>Account and registration data, contact information, and any other data except for data which is stored locally on your device.</td>
<td>Our legal, financial and compliance advisors (“Consultants”) may be exposed to certain Personal Data. The Consultants are bound by privilege obligations or confidentiality agreements and are prohibited to share any Personal Data except for providing the services we requested.</td>
</tr>
<tr>
<td>Third-party platforms</td>
<td>Registration data, Creations, and Popular Pays Marketplace activity.</td>
<td>Our services may include links to third-party websites, and integrations with third-party services. Such websites and third-party services, and any information you process, submit, transmit, store or otherwise use with such websites and third-party services, are beyond the scope of Lighttricks’ terms of use and Privacy Policy and will therefore be governed by such third-party’s terms and privacy practices and policies, and not by this Privacy Policy. Moreover, if the...</td>
</tr>
<tr>
<td>Category</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Other users</td>
<td>Creations, name, contact information. Due to the nature of the Apps and the Lightricks Feed feature, certain Personal Data available in the Apps is visible to other Lightricks users in that App, for example your username, likes and comments on other content. We will never share your photos or videos with other users unless you actively choose to do so.</td>
<td></td>
</tr>
<tr>
<td>Subsidiaries and affiliated companies</td>
<td>All data except for data which is stored locally on your device. We may share Personal Data, internally within our group or in the event of a corporate transaction (e.g., sale of a substantial part of our business, merger, consolidation or asset sale). In the event of the above, our affiliated companies or acquiring company will assume the rights and obligations as described in this Policy.</td>
<td></td>
</tr>
<tr>
<td>Third parties, authorities, security providers,</td>
<td>Any data except for data which is stored locally on your device, depending on the purpose and needs. For protecting rights and safety of our services and Apps, we may share Personal Data with others if we believe in good faith that this will help protect the rights, property or personal safety of users or individuals, or any members of the general public. This will include legal and law enforcement purposes, meaning, in response to a verified request relating to terror acts, criminal investigations or alleged illegal activity or any other activity that may expose us, you, or any other user to legal liability, and solely to the extent necessary to comply with such purpose. Such disclosure or access may occur if we believe in good faith that: (a) we are legally compelled to do so; (b) disclosure is appropriate in connection with efforts to investigate, prevent, or take action regarding actual or suspected illegal activity, fraud, or other wrongdoing; or (c) such disclosure is required to protect our legitimate business interests, including the security or integrity of our services.</td>
<td>governmental agencies, or authorized third parties.</td>
</tr>
</tbody>
</table>

When we share information with service providers and partners, we ensure they only have access to such information that is strictly necessary for us to provide the services. These parties are required to secure the data they receive and to use the data for pre-agreed purposes only while ensuring compliance with all applicable data protection regulations (such service providers may use other Non-Personal Data for their own benefit).
8. USER RIGHTS

We acknowledge that different people have different privacy concerns and preferences. Our goal is to be clear about what information we collect so that you can make meaningful choices about how it is used. We allow you to exercise certain choices, rights, and controls in connection with your information. Depending on your relationship with us, your jurisdiction and the data protection laws that apply to you, you have the right to control and request certain limitations or rights to be executed.

For detailed information on your rights and how to exercise your rights, please see the Data Subject Request Form (“DSR”) form available here and send it to our DPO: dpo@lightricks.com.

Further, certain rights are available within the App: you may correct, revise and delete information from the App settings at any time, any consent provided may be easily withdrawn, and you may opt-out from certain features and tracking, therefore we recommend you use the technical solutions we have provided you with to exercise your rights.

9. DATA RETENTION

In general, unless a different retention period is described above, we retain the Personal Data we collect for as long as it remains necessary for the purposes set forth above, when permissible by law or regulation, or until you express your preference to opt-out, where applicable.

Other circumstances in which we may retain your Personal Data for longer periods of time when permissible by law or regulation include: (i) where we are required to do so in accordance with legal, regulatory, tax, or accounting requirements, or (ii) for us to have an accurate record of your dealings with us in the event of any complaints or challenges, or (iii) if we reasonably believe there is a prospect of litigation relating to your Personal Data.

Please note that except as required by applicable law or our specific agreements with you, we will not be obligated to retain your Personal Data for any particular period, and we are free to securely delete it or restrict access to it for any reason and at any time, with or without notice to you. If you have any questions about our data retention policy, please contact us by e-mail at: dpo@lightricks.com.

10. SECURITY MEASURES

We implement appropriate and industry-standard technical, organizational, and security measures to reduce the risks of damage to (or loss of) information, or any unauthorized access or use of information. However, these measures do not provide absolute information security. Therefore, although efforts are made to secure your Personal Data, it is not guaranteed, and you cannot expect that the services will be immune to information security risks or attacks. Also, as the security of information depends in part on the security of the computer, device or network you use to communicate with us, the security of your Personal Data depends on you as well. Please make sure to take appropriate measures to use secured networks, devices and to protect your access credentials.

Please contact us at: dpo@lightricks.com if you feel that your privacy was not dealt with properly, in a way that was in breach of our Privacy Policy, or if you become aware of a third party’s attempt to gain unauthorized access to any of your Personal Data. We will make a reasonable effort to notify you and the appropriate authorities (if required by applicable law) in the event that we discover a security incident related to your Personal Data.
11. INTERNATIONAL DATA TRANSFER

Our data servers in which we host and store the information are located globally including in the US and EU. The headquarters are based in Israel where we may access the information stored on local servers, cloud-hosting servers or other systems and platforms used. In the event that we need to transfer your Personal Data out of your jurisdiction, we will take appropriate measures to ensure that your Personal Data receives an adequate level of protection as required under applicable law. Furthermore, when Personal Data that is collected within the European Economic Area ("EEA"), United Kingdoms or Swiss, is transferred outside of such jurisdiction, to a country that has not received an adequacy decision from the European Commission or the ICO, we will take necessary steps in order to ensure that sufficient safeguards are provided during the transferring of such Personal Data, in accordance with the provision of the EU, UK or Swiss Standard Contractual Clauses. Thus, we will obtain contractual commitments or assurances from the data importer to protect your Personal Data, using contractual protections that regulators have pre-approved to ensure your data is protected.

12. ELIGIBILITY AND CHILDREN PRIVACY

The services are not intended for use by children (the phrase "child" shall mean an individual that is under the age defined by applicable law), and we do not knowingly process children's information. We will discard any information we receive from a user that is considered a "child" immediately upon discovering that such a user shared information with us. Please contact us at: dpo@lightricks.com if you have reason to believe that a child has shared any information with us.

13. SPECIFICATIONS

i. Additional Notice to California Residents:

This section applies only to California residents. Pursuant to the California Consumer Privacy Act of 2018 ("CCPA") effective November 2020, and as amended by the CPRA, effective January 1, 2023.

Please see the CCPA Privacy Notice which discloses the categories of personal information collected, purpose of processing, source, categories of recipients with whom the personal information is shared for a business purpose, whether the personal information is sole or shared, the retention period, and how to exercise your rights as a California resident.

ii. Additional Notice to Colorado Residents:

Under the Colorado Privacy Act ("CPA") if you are a resident of Colorado, acting only as an individual or household context (and not in a commercial or employment context, as a job applicant or as a beneficiary of someone acting in an employment context), your rights with respect to your personal data are described below.

“Personal Data” as defined in the CPA means: “information that is linked or reasonably linkable to an identified or identifiable individual” and does not include any of the following: publicly available information, de-identified or aggregated consumer, and information excluded from the CPA scope, such as: Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPPA) or 42 CFR Part 2- “Confidentiality of Substance Use Disorder Patient Records”, Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or and the Driver’s Privacy Protection Act of 1994, Children’s Online

**Sensitive Data** includes (i) racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation; (ii) Genetic or biometric data that can be processed to uniquely identify an individual; or (iii) child data. We do not process or collect any sensitive data.

Under section 4 “PURPOSE, LAWFUL BASIS, AND PROCESSING OPERATIONS” of the Privacy Policy, we describe our collection and processing of personal data, the categories of personal data that are collected or processed, and the purposes. Additionally, in the Section describing the “DATA SHARING – CATEGORIES OF RECIPIENTS WE SHARE PERSONAL DATA WITH” details the categories of third-parties the controller shares for business purposes.

**Your Rights Under CPA:**

Herein below, we will detail how consumers can exercise their rights, and appeal such decision, or if we sell the personal data, or sell the personal data for advertising and how to opt-out.

| Right to Access/ Right to Know | You have the right to confirm whether and know the Personal Data we collected on you | You can exercise your right by reviewing this Privacy Policy, in case you would like to receive the Personal Data please fill in the DSR form to receive a copy of your data |
| Right to Correction | You have the right to correct inaccuracies in your Personal Data, taking into account the nature of the Personal Data and the purposes of the processing of your Personal Data. | You can exercise this right directly through your account or by filling in the DSR form |
| Right to Deletion | You have the right to delete the Personal Data, this right is not absolute and in certain circumstances we may deny such request. We may deny your deletion request, in full or in part, if retaining the information is necessary for us or our service provider(s) for any of the following reasons: (1) Complete the transaction for which we collected the Personal Data, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, fulfill the terms of a written warranty or product recall conducted in accordance with | If you would like to delete your Personal Data please fill in the DSR form |
|  |  | You do not need to create an account with us to submit a request to delete. You may also request deletion directly through the App settings without filling in the DSR form. |
federal law, or otherwise perform our contract with you;

2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;

3. Debug products to identify and repair errors that impair existing intended functionality;

4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law;

5. Comply with the law or legal obligation;

6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information’s deletion may likely render impossible or seriously impair the research’s achievement, if you previously provided informed consent;

7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;

8. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We will delete or de-identify personal information not subject to one of these exceptions from our records and will direct our processors to take similar action.

<table>
<thead>
<tr>
<th>Right to Portability</th>
<th>You have the right to obtain the personal data in a portable, and to the extent technically feasible, readily usable format that allows you to transmit the data to</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you would like to receive the Personal Data please fill in the DSR form. We will select a format to provide your Personal Data that is readily usable and should allow you to transmit the information</td>
</tr>
<tr>
<td><strong>Right to opt out from selling Personal Data</strong></td>
<td>another entity without hindrance.</td>
</tr>
<tr>
<td><strong>Right to opt out from Targeted Advertising</strong></td>
<td>You have the right to opt out of the sale of your Personal Data for the purposes of targeted advertising, sale to a third party for monetary gain, or for profiling in furtherance of decisions that produce legal or similarly significant effects concerning you or any other consumer. You may authorize another person acting on your behalf to opt out (including by technical tools and opt out signals). We do not profile you in a manner that has significant effect of you or and other consumer, therefore there isn’t an opt-out option. We do not “sell” or “share” information as most people would commonly understand that term, we do not, and will not, disclose your Personal Information or Personal Data in direct exchange for money or some other form of payment, however, we do share Personal Information or Data for analytic and marketing purposes, including targeted advertising, when we promote our Apps or Services. In most cases we obtain Personal Data, or Personal Information collected automatically from our Apps and your actions therein, and combine it with your actions on other of our Apps, if applicable, however not with third party apps.</td>
</tr>
<tr>
<td><strong>Right to opt out from Profiling</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Right to Appeal</strong></td>
<td>If we decline to take action on your request, we shall so inform</td>
</tr>
</tbody>
</table>
you without undue delay, within 45 days of receipt of your request. The notification will include a **justification** for declining to take action and instructions on **how you may appeal**.

| Duty not to violate the existing laws against discrimination or non-discrimination | Such discrimination may include denying a good or service, providing a different level or quality of service, or charging different prices. | We do not discriminate our users. |

**How to Submit a Request Under CPA?**

Only you, or someone legally authorized to act on your behalf, may make a request to **know** or **delete** related to your Personal Data. If the DSR is submitted by someone other than the consumer about whom information is being requested, proof of authorization (such as power of attorney or probate documents) will be required.

We will respond to your request within 45 days after receipt of a verifiable consumer request and for no more than twice in a twelve-month period. We reserve the right to extend the response time by an additional 45 days when reasonably necessary and provided consumer notification of the extension is made within the first 45 days. If we refuse to take action on a request, you may **appeal our decision** within a reasonable period time by contacting us at dpo@lightricks.com and specifying you wish to appeal. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, you may submit a complaint as follows: Colorado AG at [https://coag.gov/file-complaint/](https://coag.gov/file-complaint/)

If you have an account with us, we may deliver our written response to that account or via email at our sole discretion. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. You do not need to create an account for submitting a request.

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

**iii. Additional Notice to Virginia Residents:**

Under the Virginia Consumer Data Protection Act, as amended (“VCDPA”) if you are a resident of Virginia acting in an individual or household context (and not in an employment or commercial context), you have the following rights with respect to your Personal Data.

The VCDPA defined “**Personal data**” as detailed above under “Additional Notice to Colorado Residents”.

The VCDPA requires us to discloses the Categories of data processing and the purpose of each category, as detailed in Section 4 “PURPOSE, LAWFUL BASIS, AND PROCESSING OPERATIONS” of the Privacy
Policy, the categories of data shared and the third parties with whom it is shared, as detailed in the “DATA SHARING – CATEGORIES OF RECIPIENTS WE SHARE PERSONAL DATA WITH” Section. Disclosure of sale of data or targeted advertising are detailed in the User Rights Section above, and in the DSR Form. Further, the table above under “Additional Notice to Colorado Residents” details the rights you have under VCDPA and how you may exercise your rights.

How to Submit a Request Under VCDPA?

We shall respond to your request within 45 days of receipt. We reserve the right to extend the response time by an additional 45 days when reasonably necessary and provided consumer notification of the extension is made within the first 45 days. If we refuse to take action on a request, you may appeal our decision within a reasonable period time by contacting us at dpo@lightricks.com and specifying you wish to appeal. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, you may submit a complaint as follows: Virginia Attorney General at https://www.oag.state.va.us/consumercomplaintform

We shall provide information in response to your request free of charge, up to twice annually, unless requests are manifestly unfounded, excessive or repetitive. If we are unable to authenticate your request using commercially reasonable efforts, we may request additional information reasonably necessary to authenticate you and your request. If we cannot authenticate you and your request, we will not be able to grant your request.

iv. Additional Notice to Connecticut Residents:

Under the Connecticut Data Privacy Act, Public Act. No. 22-14 (the “CDPA”) if you are a resident of Connecticut, acting in an individual or household context (and not in a commercial or employment context or as a representative of business, non-profit or governmental entity), your rights with respect to your personal data are described below.

“Personal data” means any information that is linked or reasonably linkable to an identified or identifiable individual. It does not include de-identified data or publicly available information. If further does not include information excluded from the scope such as: HIPAA, GBPA, non-profit entities, higher education, employment data and FCRA, Driver’s Privacy Protection Act of 1994, Family Educational Rights and Privacy Act, Farm Credit Act.

The categories of personal data processed, purpose of processing, are as detailed in Section 4 “PURPOSE, LAWFUL BASIS, AND PROCESSING OPERATIONS”, categories of personal data shared with third parties, categories of third parties with whom data is shared, are detailed in the “DATA SHARING – CATEGORIES OF RECIPIENTS WE SHARE PERSONAL DATA WITH” Section. Disclosure of sale of data or targeted advertising are detailed in Section 8 "USER RIGHTS", and in the DSR Form.

Instructions on how to exercise your rights are detailed in the table above under “Additional Notice to Colorado Residents” details the rights you have under CDPA and how you may exercise your rights. In addition to the table above, under CDPA you also have the right to withdraw consent which shall be provided within 15 days.

How to Submit a Request Under CDPA?

We shall respond to your request within 45 days of receipt. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of requests and we inform you of such extension within the initial 45 day response period, together with the reason for the extension.
If we decline to take action on your request, we shall so inform you without undue delay, within 45 days of receipt of your request. The notification will include a justification for declining to take action and instructions on how you may appeal. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, you may submit a complaint to the Connecticut Attorney General at link: https://www.dir.ct.gov/ag/complaint/ or (860) 808-5318.

We shall provide information in response to your request free of charge, up to twice annually, unless requests are manifestly unfounded, excessive or repetitive. If we are unable to authenticate your request using commercially reasonable efforts, we may request additional information reasonably necessary to authenticate you and your request. If we cannot authenticate you and your request, we will not be able to grant your request.

v. Additional Notice to Utah Residents (Effective January 2024):

Under the Utah Consumer Privacy Act (the “UCPA”) if you are a resident of Utah, acting in an individual or household context (and not in a commercial or employment context) your rights with respect to your personal data are described below. The UCPA defined “Personal Data” as detailed above under “Additional Notice to Colorado Residents”.

The categories of personal data processed, purpose of processing, are detailed in Section 4 “PURPOSE, LAWFUL BASIS, AND PROCESSING OPERATIONS”, categories of personal data shared with third parties, categories of third parties with whom data is shared, are detailed in the “DATA SHARING — CATEGORIES OF RECIPIENTS WE SHARE PERSONAL DATA WITH” Section. Disclosure of sale of data or targeted advertising are detailed in Section 8 "USER RIGHTS", and in the DSR Form.

Further, the table above under “Additional Notice to Colorado Residents” details the rights you have under CDPA and how you may exercise your rights.

vi. Additional Notice to Nevada Residents:

Nevada law allows Nevada residents to opt out of the sale of certain types of personal information. Subject to several exceptions, Nevada law defines “sale” to mean the exchange of certain types of personal information for monetary consideration to another person. We currently do not sell personal information as defined in the Nevada law. However, if you are a Nevada resident, you still may submit a verified request to opt out of sales and will record your instructions and incorporate them in the future if our policy changes. You may send opt-out requests to us at dpo@lightricks.com or through the DSR Form.

vii. Additional Notice to Brazil Residents:

We have created this section specifically for users in Brazil. Users in Brazil have certain privacy rights as specified under Brazilian law, including the Lei Geral de Proteção de Dados Pessoais (“LGPD”). Our Privacy Policy and the privacy controls we offer to all users are in line with these laws—this notice makes sure we cover the Brazil-specific requirements. For example, all users can request a copy of their data, request deletion, and control their privacy settings in the app.

Data Controller information is available above in Section 2.

The lawful basis under the LGPD is Contract (complying with the obligations of the agreement we have entered), Legitimate Interest (we have the right, the legitimate interest, to do so), Consent (we have asked your permission) and Legal Obligations. The Tables in Section 4 detail the lawful basis for processing each data set.