

## Onelight Apps Privacy Policy

This Privacy Policy describes the ways we collect, store, use and manage any Personal Data you provide to us or we collect in connection with your use of our Apps and Websites.

BY CLICKING “I AGREE” OR BY USING OUR APP OR WEBSITE YOU AGREE TO THIS PRIVACY POLICY and the processing of your Personal Data in the manner provided in this Policy. If you do not agree to the terms of this Privacy Policy, please do not use the Apps and Websites.

### 1. Definitions

“**Policy**” means this Onelight Apps Privacy Policy.

“**We**”, “**our**” or “**us**” means Onelight Apps entity specified in the applicable app store or on the Website.

“**You**”, “**your**” means you as a user of our Apps or Websites.

“**App**” means a mobile application developed by us and available through Google Play or Apple App Store.

“**Website**” means our website on which this Policy appears.

“**Terms**” means [Onelight Apps Terms of Use](#).

“**Personal Data**” means information that can be used to identify you as an individual, like your first and last name, email address, username, usage data and so on. Personal Data does not include information that has been anonymized such that it does not allow for your identification. If you cannot be identified (e.g., when Personal Data has been aggregated and anonymized), then this Policy does not apply.

### 2. What Data We Collect and How We Do That

When you visit our Websites, use our Apps or contact us directly we collect and process your Personal Data. The ways we collect it can be broadly categorized into the following:

#### Information you provide to us directly

When you use some parts of our Apps we might ask you to provide Personal Data to us. For example, you will provide your email address when you contact us with questions or request support. Certain Apps need access to your photos located on your device (if you have granted us permission to access your photos). You may upload your photos (including their metadata) using certain features of our Apps and specify your email address or Instagram name. We process only specific photos you chose to modify using an App. We do not collect your Instagram photos or photo albums.

#### Information we collect automatically

We may automatically collect certain information about the devices you use to access the Apps and Websites. As described further below, we may collect and analyze (a) device information and identifiers such as IP addresses, location information (by country and city), unique device identifiers, Google Advertising ID, Apple ID for Advertising, IMEI and TCP/IP address, browser types, screen resolution, browser language, operating system, mobile device carrier information, and (b) information related to the ways in which you interact with the Apps and Websites, such as referring and exit web pages and URLs, platform type, the number of clicks, content viewed, statistical information about the use of the Apps and Websites (e.g. features you use; screens you viewed, navigation paths between pages or screens, the actions you take; the date and time you used the Apps and Websites, the frequency of your use of the Apps and Websites), error logs, and other similar information.

As described further below, we may use third-party web and mobile analytics services and technologies (such as [Google Analytics](#), [Facebook Analytics](#), [Amplitude](#), [Firebase](#), [AppStore Analytics](#), etc.), including cookies and similar tools, to assist in collecting this information. The information collected by various analytics technologies described in this section above will be disclosed to or collected directly by these service providers, who use the information to evaluate your use of the Apps and Websites, including by analyzing usage trends, assisting with fraud prevention, and providing certain features to you.

Some of this information is collected using cookies and similar tracking technologies.

### **Cookies and similar tracking technologies**

We do not use our (first-party) cookies.

Mobile devices may use other tracking files which are similar to cookies (for example iOS devices use Apple's Advertising Identifier and Identifier For Vendor, and Android devices use Google's Advertising ID).

We also use third-party software development kits SDKs, which are blocks of code provided by our analytics or advertising partners that we may instal in our Apps. SDKs help these third parties and us understand how you interact with our Apps and collect certain information about the device and network you use to access the Apps. SDKs may collect above-mentioned identifiers associated with your device or our Apps. Please refer to our partners' privacy and data sharing statements found on their respective websites for more information.

To express the choice not to have information about your use of mobile ads used for interest-based advertising purposes on your iOS mobile device, you should follow this path: Launch "Settings" > Tap on "Privacy" and scroll down and tap on "Advertising" > Toggle on "Limit Ad Tracking." To block Android ID on your Android device, you should follow this path: Launch "Settings" > Tap on Google > Ads and then turn on 'Opt out of Ads Personalization'. You can also reset your advertising ID from there by tapping "Reset Advertising Identifier."

If you opt-out of having your information collected and used by us and our third-party advertising partners for interest-based advertising purposes, you will continue to receive ads, but such ads will not be tailored to your specific interests based on web viewing data collected from your device.

### **Information we get from third parties**

We might collect Personal Data about you from third parties like Instagram. For example, in certain cases you can connect to our Apps through Instagram's API. If you connect to us through Instagram, we will collect, store, and use in accordance with this Policy information you agreed that Instagram could provide to us through their API (e.g., your username, number of followers, account type, number of entries, version of the application, etc.).

## **3. Third Parties Processing Your Personal Data**

This Policy does not cover the collection, processing, storage or use of your Personal Data, by Instagram, Adobe, Apple, Google or any other third parties. We do not control when or how third parties collect, process, store or use your Personal Data. Please refer to the privacy policies of third parties in order to learn and understand how and when they use your information.

## **4. Legal Grounds to Process Personal Data**

If you are an individual in the European Economic Area (EEA) the following provisions of

this section apply to you.

Where we collect Personal Data, we will only process it when we have the legal basis for the processing set out in applicable data protection laws. Such legal bases are:

- **The performance of a contract.** We may process your Personal Data where we need to take steps at your request prior to entering into a contract or where it is necessary for the performance of a contract.
- **The legitimate interests.** Your Personal Data may be processed when we, other companies in our group of companies or third parties have a business or commercial reason to process your Personal Data.
- **A legal obligation.** Various laws and regulations may impose certain obligations on us. To comply with them we have to process your Personal Data.
- **Your consent.** In certain limited cases we process your Personal Data based on your consent, for example, when it is required for direct marketing purposes and you have not used our Apps or have not expressed interest in them.

## 5. How We Use Personal Data

Our processing of your Personal Data is necessary for us to provide you with the Apps and Websites. If we do not process your Personal Data, we may be unable to provide you with all or some features of the Apps.

We use your Personal Data for a number of purposes, which may include the following:

Use of your Personal Data	Legal basis (for EEA)
To operate our Apps and Websites, ensure they work as intended and deliver the services you have requested.	Performance of a contract Legitimate interest
Authenticate you when you log in using third-party log-in services (e.g. Instagram).	Performance of a contract Legitimate interest
To support you, including assisting with the resolution of technical or other issues relating to the Apps and Websites.	Performance of a contract
To enhance our Apps and Websites, test and develop new features and carry out analysis of our Apps and Website so that we can optimize your user experience and provide you and other users with more efficient tools and features.	Legitimate interest
To analyze and aggregate data, to prepare statistics, in particular, to produce aggregated and anonymized analytics and reports, which we may use internally or share publicly or with third parties.	Legitimate interest
To display advertisements to you.	Legitimate interest
To manage our relationship and communicate with you (including by push notifications). This may include: <ul style="list-style-type: none"> <li>● operational and transactional communications about or in relation to changes to our Apps, our services, features, security updates, assistance with using our Apps, or requests for feedback;</li> <li>● survey requests, feedback collection and follow-up communication if these Terms or an App's use has been terminated or suspended;</li> </ul>	Performance of a contract Legitimate interest

<ul style="list-style-type: none"> <li>• providing you with the information you have requested from us or information we are required to send to you.</li> </ul> <p>These communications are part of the services we provide to you through the Apps and in most cases you will not be able to opt out of them. If an opt-out is available, you will find that option within the communication itself or in the App's settings.</p>	
To promote and drive engagement with the Apps and Websites.	Legitimate interest
To send marketing communications that may be of specific interest to you. These communications are aimed at driving engagement and maximizing what you get out of the Apps, including information about new Apps, newsletters, product offers, and promotions we think may be of interest to you. You may opt out of receiving marketing communications from us managing notifications settings on your mobile device.	Legitimate interest Your consent
To prevent, detect and report crime, protect you, other users and us, for example, by ensuring network and information security, mitigating security risks, detecting and preventing any fraudulent or malicious activity, and make sure that everyone is using our Apps and Websites fairly and in accordance with the Terms.	Legal obligation Legitimate interest Performance of a contract
To perform legal duties, responsibilities, and obligations; and to comply with any laws and regulations that apply to us.	Legal obligation
To exercise our rights set out in the Terms or other agreements with you.	Performance of a contract
To disclose information to companies in our group of companies following a restructure or for internal administrative purposes.	Legitimate interest

We may aggregate and/or de-identify information collected through the Apps and Websites. We may use de-identified and/or aggregated data for any purpose, including without limitation for research and marketing purposes.

## 6. How We Can Share Your Personal Data

We do not share your photos with third parties with the exception of uploading them to your Instagram profile to provide you with the service you requested by using the App.

There will be times when we may need to share your Personal Data with third parties. We may disclose your Personal Data to:

- Other companies in our group of companies;
- Third-party service providers and partners who assist us in the provision of the Apps and Websites, for example, (a) those who support delivery of or provide certain features in connection with the Apps and Websites; (b) providers of analytics and

- measurement services; (c) providers of technical infrastructure services; (d) providers of customer support services; (e) those who facilitates conducting of surveys; (f) advertisers; or (g) those who market or promote our Apps and Websites;
- Regulators, law enforcement agencies, government bodies, courts, fraud prevention agencies, or other third parties, where we think it is necessary to comply with applicable laws or regulations, or to exercise, establish or defend our legal rights (where possible and appropriate, we will notify you of this type of disclosure);
  - Professional advisors, such as lawyers, auditors, etc. where necessary in the course of the professional services that they render to us;
  - An actual or potential buyer (and its agents and advisers) in connection with an actual or proposed purchase, merger or acquisition of any part of our business; and/or
  - Other persons where we have your consent.

## **7. Data Retention**

Some data you can delete whenever you like, some data is deleted automatically, and some data we retain for longer periods of time when necessary. When the data is being deleted, we make sure that your data is safely and completely removed from our servers or retained only in anonymized form.

### **Information retained until you remove it**

If you are connected to our App by using your Instagram account you can stop sharing the information from Instagram with us by removing our access to this service.

### **Information for marketing communications**

If you have not opted-out or have consented (as the case may be) to receive marketing communications from us, we retain information about your marketing preferences for a reasonable period of time from the date you last used or expressed interest in our Apps or Websites.

### **Information retained for extended time periods for limited purposes**

Sometimes business and legal requirements oblige us to retain certain information, for specific purposes, for an extended period of time. Reasons we might retain some data for longer periods of time include:

- To ensure that the Apps and Websites are available to you and other users.
- To protect you, other persons, and us from fraud, abuse, illegal activity and unauthorized access, for example, when you suspect someone is committing fraud.
- To comply with tax, anti-money laundering and other financial regulations or to carry out accounting.
- To facilitate dispute resolution.
- To meet any comply with applicable law, regulation, legal process or enforceable governmental request, or when we are required to enforce the Terms, including investigation of potential violations.
- If you have directly communicated with us, for example, through a customer support channel or providing feedback or a bug report.

## **8. Your Rights**

You have the following rights with respect to your Personal Data that we process:

- Right to opt out. You have the right to opt out of marketing-related communications

we may send you via push notification by changing the settings on your mobile device.

- Right to revoke App permissions. You have the right to revoke any permissions you previously granted to us, such as permission to access your photos, through the settings on your mobile device.

When the EU General Data Protection Regulation (GDPR) applies to our relations (e.g. you are located in the EU), you have the following rights with respect to your Personal Data that we process:

- Right to access. You have the right to access (and obtain a copy of, if required) your Personal Data.
- Right to rectification. You have the right to update your Personal Data or to correct any inaccuracies.
- Right to erasure. You may have the right to request that we delete your Personal Data in certain circumstances, such as when it is no longer necessary for the purpose for which it was originally collected.
- Right to restriction of processing. You may have the right to request to restrict the use of your Personal Data in certain circumstances, such as when you have objected to our use of your Personal Data but we need to verify whether we have overriding legitimate grounds to use it.
- Right to data portability. You have the right to transfer your Personal Data to a third party in a structured, commonly used and machine-readable format, in circumstances where the Personal Data is processed with your consent or by automated means.
- Right to object. You may have the right to object to the use of your Personal Data in certain circumstances, such as the use of your Personal Data for direct marketing.
- Right to complain. If you are not happy with how we are processing your Personal Data, please let us know by sending an email to [privacy@onelightapps.io](mailto:privacy@onelightapps.io). We will review and investigate your complaint, and try to get back to you within a reasonable time frame. You have the right to complain to your local data protection authority. This right may not be available to you if there is no authority dealing with data protection in your country..

You can exercise your rights at any time by sending an email to [privacy@onelightapps.io](mailto:privacy@onelightapps.io). We may require evidence of and be satisfied as to your identity before we take any requested action.

## **9. Security Measures**

We have implemented technical, physical, and organizational security measures to protect against the loss, misuse, and/or alteration of your information. These safeguards vary based on the sensitivity of the information that we collect and store. However, we cannot and do not guarantee that these measures will prevent every unauthorized attempt to access, use, or disclose your information since despite our efforts, no Internet and/or other electronic transmissions can be completely secure.

## **10. International Data Transfers**

When we process and share data, it may be transferred to, and processed in, countries other than your country. These countries may have laws different to what you are used to. Where Personal Data is processed in another country, we put safeguards in place to ensure your Personal Data remains protected.

For individuals in the European Economic Area (EEA), this means that your data may be transferred outside of the EEA. Where your Personal Data is transferred outside the EEA, it will be transferred to countries where we have compliant transfer mechanisms in place to protect your Personal Data, in particular, by implementing the European Commission's Standard Contractual Clauses to the contracts with the entities the data is transferred to.

## **11. Information Concerning Children**

The Apps and Websites are not directed at children under the age of 13. If we become aware that we have collected personal information (as defined by the US Children's Online Privacy Protection Act) from children under the age of 13, or personal data (as defined by the EU GDPR) from children under the age of 16, we will take reasonable steps to delete it as soon as practicable.

## **12. Third-Party Links and Services**

The Apps and Websites may contain links to third-party websites, apps, plug-ins and other services. If you choose to use these sites or features, you may disclose your information not just to those third-parties, but also to their users and the public more generally depending on how their services function. We are not responsible for the content or privacy practices of such third party websites or services. The collection, use and disclosure of your information will be subject to the privacy policies of the third party websites or services, and not this Privacy Policy. We encourage you to read the privacy statements of each and every site you visit.

## **13. Modifications**

We may modify or revise this Policy at any time by posting the amended Policy. Please check the most current Policy.

## **14. Privacy Related Inquiries**

If, for any reason, you are concerned with the way that we may be using your Personal Data, you have questions about the privacy aspects of the Apps or Websites, please, contact us at [privacy@onelightapps.io](mailto:privacy@onelightapps.io).

For users in the EU, we have appointed Onelight Apps CY Ltd. as our EU representative. You can address any questions or concerns you have either as described above or to our EU representative as follows:

Onelight Apps CY Ltd.  
Spyrou Araouzou 165  
Lordos Waterfront Office 402,  
Limassol, 3036 Cyprus.

## **15. California Privacy Rights Notice**

This PRIVACY NOTICE FOR CALIFORNIA RESIDENTS supplements the information contained in our Privacy Policy This PRIVACY NOTICE applies solely to visitors, users, and others who reside in the State of California.

Although we are not doing business in California for the purposes of the California Consumer Privacy Act of 2018 ("CCPA") (Civil Code Section § 1798.100 et seq.), this notice

is adopted to comply with the CCPA. Any terms defined in the CCPA have the same meaning when used in this notice.

### Information We Collect

Our Apps and Websites may collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device, including but not limited to identifying information (collectively, “personal information”). In particular, we have collected the following categories of personal information from consumers within the last twelve (12) months:

Category	Examples	Collected
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.	NO
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and	NO



	voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data.	Physical location or movements.	NO
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	YES
I. Professional or employment-related information.	Current or past job history or performance evaluations.	NO
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO

### **Disclosures of Personal Information for a Business Purpose**

In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

- Category A: Identifiers.
- Category F: Internet or other similar network activity.

### **Sales of Personal Information**

We do not sell the personal information of consumers.

In the preceding twelve (12) months, we have not sold any personal information.

### **Your Rights and Choices under the CCPA**

The CCPA provides consumers, which are California residents, with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

### **Access to Specific Information and Data Portability Rights**

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we received and

confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing (a) sales, identifying the personal information categories that each category of recipient purchased; and (b) disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

### **Deletion Request Rights**

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Debug products to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
- 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.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

### **Exercising Access, Data Portability and Deletion Rights**

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Visiting “Contact us” page of an App or Website,
- Emailing us at [privacy@onelightapps.io](mailto:privacy@onelightapps.io),

- Mailing your request to us at the mailing address indicated in Section 1 of this Policy.

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

### **Response Timing and Format**

We will endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

If you are our current customer, we will deliver our written response to the contact information we have on file for you (if we have any). Otherwise we will deliver our written response electronically, at the email address specified in the verifiable consumer request.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily usable and should allow you to transmit the information from one entity to another entity without hindrance.

We will not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

**Last updated: August 02, 2021**