

## Privacy Notice

1. Who we are
2. Scope of this Notice
3. Data collection
4. Details of data processing
5. Profiling and automated decision-making
6. Data transfers to third parties
7. Transfers to other countries
8. Data protection
9. Deletion of data
10. Your rights
11. Additional information for residents of some US states
12. Changes and updates

### Who we are

We are Skylum Software USA, Inc.. We are a corporation registered in the United States, registered at 142 W 57th St, New York, NY 10019, United States., and we are the controller of your personal data. It means that we determine what, for what purpose and how your personal data will be processed.

If you have any questions, please contact us at [ivan@skylum.com](mailto:ivan@skylum.com).

Our support will assist with any your queries. Note that we may need to request additional information from you to validate the request. Also, we do not process requests without name and contact details.

### Scope of this Notice

This Privacy Notice applies to our mobile app **imgmi (App)** and services we provide.

Our App may contain links to other websites. We are not responsible for their privacy practices. When you leave our App, please be sure to read the privacy notices and policies of those other websites.

We also knowingly do not provide services and/or process personal data of persons under the age of 16. If you are such a person, or you are his/her legal representative, please let us know by email.

### Data collection

Depending on your interactions on the App and permissions, we process the following data:

Identifiers: name, email, account name, ID, and other information you may share within registration or identifying your account.

Content: any material uploaded to the App, including any photos, videos, data, metadata, images, and any other material whatsoever.

Payment data: your banking card, details of your payment.

Transactions: products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

Interactions: your activities at the App, including browsing history, search history, and interaction with the website or advertisement.

Technical data: the type of device you use, access times, IP-address, general location information of your Internet Service Provider based on it and similar, interactions with the App.

Usually, we collect data only from you. Also, some of your data will be shared by Apple due to their practices.

### Details of data processing

<b>Purpose</b>
<b>Data</b>
<b>Legal Basis</b>
<b>Processing Time</b>

Provision and management of the services according to Terms of Use

Identifiers, Content, Payment data, Transactions, Interactions, Technical data

Terms of Use, meaning performance of the contract

If you are not registered – during interaction with the App

If you are registered – during your registration and for 3 months after it

Making services more convenient for you: customized results of the search

Identifiers, Technical data

Your consent

Until you delete these data from your account

Processing and answering your requests

Identifiers and any other data you provide or are necessary for the answer

Legitimate interest: communication between us

If you are not registered – during 1 year from the last communication

If you are registered – during your registration and for 3 months after it

Marketing, includes profiling (Section 6)

Identifiers, Content, Transactions, Interactions, Technical data

Your consent

During term of your consent

Compliance with the law (financial, content, personal data etc.)

Identifiers, Content, Payment data, Transactions, Interactions, Technical data

Legal obligation

Depending on the data and relevant law

Technical safety and prevention of illegal activities

Identifiers, Content, Interactions, Technical data

Terms of Use, meaning performance of the contract: for correction of bugs and ensuring of App's proper functioning

Legitimate interest: prevention of data breaches and other security leaks; prevention of any illegal activities and crimes

During your interaction with or registration in the App

Statistics for further development and enhancing of the App

Content, Transactions, Interactions, Technical data

Other data – only provided anonymization

Legitimate interest: detection of ineffective or unsatisfactory features and their correction, as well as development of new and better services

During your interaction with the App

Protection of interests and proceeding with claims

Any data relating to claim or proceeding which we lawfully process

Legitimate interest: protection of our rights and interests

Within the relevant proceeding and for 3 years after the final decision

## Profiling and automated decision-making

### Profiling

We create profiles only for marketing purposes based on your consent. The system analyses information about you in whole as a data complex. Please note that such information will include, depending on your option, Identifiers, Content, Transactions, Interactions, Technical data.

This way we analyze and try to predict your preferences for this or that content, goods, or services and further offer those potentially interesting specifically for you.

We do not make any decisions based on your profile. Also, we build our analytic system with principle of fairness. Still, we cannot completely exclude errors. So, please if you found any offending for you

offers let us know.

Automated decision-making

We do not use automated decision-making.

Data transfers to third parties

We do not sell your personal data, but we may transfer your personal information to some of our contractors.

Please note that if a data transfer is necessary for our agreement with you and achieving purposes specified above, we have the right to do so without your consent. We will ask you if the transfer is not necessary.

We will always ensure appropriate measures for your personal data protection according to this Privacy Notice. We also implement appropriate safeguards with these third parties to ensure that such data transfers are safe, secure and confidential.

So, we share your data:

With our contractors and partners

We share your personal data with our contractors and partners for provision of services and achievement of purposes identified above. Some of the contractors may also process your data on our behalf.

We choose our contractors and partners very carefully. We also have agreements in place with all of them and require them to operate and conduct themselves consistently with our legal and ethical obligations.

These third parties service providers include:

hosting provider;

payments system;

IT providers which help to maintain the App;

our professional advisers;

suppliers who provide certain support services for example, document production, translation;

marketing support providers.

For compliance with the law

We will disclose your personal data to third parties to the extent that it is necessary:

to comply with a governmental request, court order, or applicable law;

to prevent illegal use of our website;

to protect against claims of third parties; or

to help prevent or investigate fraud.

Transfers to other countries

The App is operated from the United States.

We may engage services suppliers in different countries. However, we always ensure a proper level of data protection and use of adequate organizational and technical measures in any case.

Data protection

We take care of your data and use appropriate technical, physical, and organizational means for their protection. These include, in particular:

Technical means: secure HTTPS protocol, encryption and backup technologies, servers in the European Union, custom licensed software.

Physical means: limited access to the premises, their round-the-clock security and video surveillance.

Organizational means: non-disclosure agreements, internal policies, and guidelines.

Deletion of data

We will delete your data completely when (*whichever happens later*):

the processing time will expire; *or*

the system will update the backup.

Also, you can always request the deletion of data or the account. Please write us for this.

We will consider the request and confirm or reject it. Further, the data will be completely deleted in 3 months (after the backup update). Within this time, we will limit processing of your data and hide it from users. Also, within this time you may restore the data writing us.

Please note that sometimes we cannot delete your data completely, e.g. when the law requires the relevant processing. Anyway, in such case, we will stop any other processing and restrict access to data.

Your rights

To exercise your rights, please write us an email. Note that we may need to request additional information from you to validate the request. Also, we do not process requests without name and contact details.

Depending on the state and legislative requirements we have from 30 to 60 days to exercise your request with the right to postpone it for 30 days more.

### **United States Residents**

Your rights vary depending on the laws that apply to you, but may include:

<u>Right</u>	<u>Description</u>	<u>Area</u>
--------------	--------------------	-------------

Right to access		
-----------------	--	--

	You can request an explanation of the processing of your personal data.	
--	---	--

		California, Virginia, Ohio, Colorado, Nevada, Massachusetts, Minnesota, North Carolina, New York, Pennsylvania, Delaware, Utah
--	--	--

Right to rectification		
------------------------	--	--

	You can change the information if it is inaccurate or incomplete.	
--	---	--

		California, Virginia, Colorado, Nevada, Delaware, Massachusetts, Minnesota, North Carolina, New York
--	--	--

Right to deletion		
-------------------	--	--

	You can send us a request to delete your personal data from our systems.	
--	--	--

		California, Virginia, Ohio, Colorado, Massachusetts, Minnesota, North Carolina, New York, Pennsylvania, Utah
--	--	--

Right to restriction		
----------------------	--	--

	You may partially or completely prohibit us from processing your personal data.	
--	---	--

		California, Massachusetts, New York
--	--	-------------------------------------

Right to portability		
----------------------	--	--

	You can request all the data that you provided to us, as well as request to transfer data to another controller.	
--	--	--

		California, Virginia, Ohio, Colorado, Massachusetts, Minnesota, North Carolina, New York, Utah
--	--	--

Right to Opt-Out		
------------------	--	--

	You can prohibit the sharing or selling of your data.	
--	---	--

		California, Virginia, Ohio, Nevada, Massachusetts, Minnesota, North Carolina, New York, Pennsylvania, Delaware, Colorado, Utah
--	--	--

Right against automated decision making		
---	--	--

	You have the right not to be subject to a decision based solely on automated means, if the decision produces legal effects concerning you or significantly affects you in a similar way.	
--	--	--

		California, Virginia, Colorado, Massachusetts, Minnesota, North Carolina, New York
--	--	--

Right to lodge a complaint		
----------------------------	--	--

	If your request was not satisfied, you can file a complaint to the regulatory body.	
--	---	--

By default		
------------	--	--

### **European Union and other states residents**

You, as a data subject, have the following rights:

Access the information: You can request an explanation of the processing of your personal data.

Rectification: You can request correction of any wrong or incomplete data we process about you.

Portability: You can request all the data that you provided to us, as well as request to transfer data to another controller.

Withdraw a consent: For processing that you have previously consented to, you can always withdraw your consent and we will stop processing it. Usually, you may do it in the way you agreed: by deleting non-obligatory data from the account or changing configurations. Also, you always may send us an email request.

Object to processing: Where the processing is based on the public or legitimate interest, you may object at any time to such processing.

Restrict processing: You may partially or completely prohibit us from processing your personal data.

To be forgotten: You can send us a request to delete your personal data from our systems.

File complaints: If your request was not satisfied, you can file a complaint to the regulatory body.

Additional information for residents of some US states

## Legislation of the California state

We are posting information here for California residents to provide you with more information about the law and your privacy rights under the California Consumer Privacy Act ("CCPA") and the California Privacy Rights Act.

Opting out of selling data for direct marketing purposes. California law allows its residents to find out which organizations received their personal information for marketing purposes and the categories of information disclosed. You can submit a request to receive such data — contact us.

Note that opting out of selling data for direct marketing purposes does not prevent us from disclosing personal information for purposes other than direct marketing purposes. The data we process and share may include your name, address, email address and telephone number.

Juvenile policy. Data controller must not sell the personal information of data subjects if it has actual knowledge that the subject is less than 16 years old, unless the subject (in case of age from 13 to 16 years old) or his parent/guardian (in case if the subject is less than 13 years old) did not give permission to sell the personal information of the subject. Data controller that deliberately ignores the subject's age will be considered one that knows the subject's actual age. This right may be referred to as "opting out of the sale of data". Data controller who has not received consent to sell personal information of a minor subject is prohibited from selling personal information unless the subject subsequently provides explicit consent.

The right to know what data is being collected: you have the right to request us to disclose to you certain information about the personal information we have collected, processed, disclosed and sold about you in the past 12 months. This includes a request for any or all of the following information:

the categories of personal information collected about you;

the categories of sources from which we obtained personal information;

the categories of your personal information that we have sold or disclosed for a commercial purpose;

the categories of third parties to whom your personal information has been sold or disclosed for commercial purposes;

our business or commercial purpose for collecting/selling your personal information; and specific pieces of personal information we have collected about you.

The right to data portability: you have the right to request a copy of the personal information we have collected and stored about you over the past 12 months.

Right to deletion: You have the right to request us to delete the personal information we have collected from you and stored, subject to certain exceptions. Note that if you request the deletion of personal information, we may refuse your request or retain some of your personal information if it is necessary for us or our service providers to:

- completing the transaction for which the personal information was collected, providing a product or service requested by you or reasonably expected in the context of our current business relationship, or otherwise performing a contract between you and the data controller;

detecting security breaches, protecting against malicious, unscrupulous, fraudulent or illegal activities; or harassment of persons responsible for such activities;

debugging to identify and fix bugs that break existing planned functionality;

exercising the right to freedom of speech, ensuring the rights of another subject to exercise their right to freedom of speech or other rights provided for by law;

compliance with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (beginning with Section 1546) of Section 12 of Part 2 of the Criminal Code;

conducting public or peer-reviewed scientific, historical or statistical research in the public interest, complying with all other applicable ethics and data protection laws, where deletion of information could make it impossible or seriously impair such research if you have provided informed consent;

provide for exclusively internal use that reasonably meets your expectations based on the nature of your relationship with us;

fulfillment of legal obligations;

use personal information internally in a lawful manner consistent with the context in which you provided it.

Right to Opt Out/Consent to the Sale of Personal Information: You have the right to object to the sale of your personal information. You also have the right to consent to the sale of personal information.

However, we do not sell your personal information.

Right to non-discrimination: You have the right not to be treated discriminatorily by us for exercising your rights regarding your data under the CCPA. Unless permitted by law, we will not:

- refuse to provide goods or services.

set other prices or tariffs for goods/services, including by providing discounts (or other benefits), or imposing fines.

provide goods or services of a different level or quality.

offer you a different price or rate for goods or services.

You can exercise these rights at any time — contact us.

The consumer privacy law provides for some specific requirements related to the exercise of these data protection rights. Given them, we can:

- respond to your request within 45 days of receiving your request;

provide you with personal information that we have collected about you no more than twice in 12 months (categories and specific sections of personal information collected, purposes and sources of collection, categories of third parties to which personal information is transferred);

not provide you with personal information if we cannot verify your identity. You must provide us with sufficient information so that we can verify you as the subject we are collecting data about. That being said, we consider requests made through your account to be sufficiently verified;

not transfer your personal information to another legal entity.

In addition, we have the right to retain personal information after receiving a deletion request, as permitted by consumer privacy law (for example, to detect security breaches, correct errors, comply with legal obligations, complete transactions).

You will not be discriminated against if you choose to exercise your rights under the CCPA. We are accessible to people with disabilities who can contact us by email and request an alternative Notice format.

### **Legislation of the state of Virginia**

We provide information here for Virginians to assure you with more information about the law and your privacy rights under the Virginia Consumer Data Protection Act.

This law obliges some data controllers to provide subjects with the ability to access and control the personal data that the operator collects about them.

Juvenile policy. Controllers and processors of personal data on behalf of the operator who comply with the Children's Online Privacy Protection Act (COPPA) requirement to verify parental consent will be deemed to comply with any obligation to obtain parental consent under the Consumer Privacy Act (VCDPA). A parent or legal guardian may exercise rights on behalf of a minor subject in relation to the processing of personal data belonging to a minor subject.

The right to non-discrimination. Data Controller may not process personal data in violation of state and federal anti-discrimination laws or discriminate against a subject for exercising rights under the VCDPA.

Access request. Data controllers are required to establish and describe in the Notice one or more safe and secure means for subjects to submit requests to exercise their rights. The method used should take into account how customers typically interact with the controller, the need for secure and reliable transmission of such requests, and the controller's ability to validate requests. Data controllers are prohibited from requiring a subject to create a new account to exercise their rights, but may require a subject to use an existing account.

Request response time. Data controller is obliged to respond to requests from subjects within 45 days. This period may be extended once for 45 additional days, subject to certain requirements.

Free provision of information. Data controllers are obliged to provide information in response to the request of the subject free of charge, no more than twice a year for one subject. The Data Controller may charge the subject a reasonable fee or refuse to comply with the request if the requests are manifestly unfounded, excessive or repetitive, but it is the responsibility of the Controller to demonstrate the manifestly unreasonable, excessive or repetitive nature of the request.

### **Legislation of the state of Colorado**

We are posting information here for Colorado residents to provide more information about the laws and privacy rights provided by the Colorado privacy law.

Juvenile policy. Data controller shall not process personal data of minors without prior consent from their parent or legal guardian

Access request. Subjects may exercise their rights by submitting a request, by the method specified by the controller in the Notice. The method must take into account:

- the ways in which subjects typically interact with data controller;

the need for secure and reliable communication related to the request;

the controller's ability to identify the identity of the subject making the request.

Data controllers are prohibited from requiring a subject to create a new account to exercise their rights, but may require a subject to use an existing account.

Request response time. Data controller is obliged to respond to requests from subjects within 45 days.

Data controller must inform the subject of any action taken on the request within 45 days. Under certain circumstances, this 45-day response period may be extended by an additional 45 days.

Free provision of information. Data controllers are obliged to provide the requested information free of charge once a year. For repeated requests within a 12-month period, the operator may charge an additional amount.

Justification for inaction. If the data controller does not take action at the request of the subject, then he must inform the subject within 45 days after receiving the request about the reasons for not taking action and instructions for appealing the decision.

Refusal to complete the request. Data controller is not required to comply with a request to exercise any of the subject's rights if the data controller cannot authenticate the request using reasonable efforts and may request the provision of additional information reasonably necessary to authenticate the request.

Right to appeal the decision. Data controller must establish an internal process by which subjects can appeal a denial of action at the subject's request. If the subject wishes to appeal the decision, he must do so within a reasonable period of time after the data controller notifies him that he is denying the request. The appeals process should be visible and easy to use.

Response to an appeal. Data controller must inform the subject of the outcome of the appeal and provide a written explanation of the reasons in support of the outcome within 45 days of receipt of the appeal. This 45 day period may be extended for another 60 days under certain circumstances.

### **Legislation of the state of Delaware**

We are posting information here for Delaware residents to provide more information about laws and privacy rights provided by the Delaware Online Privacy and Protection Act.

Advertising addressed to children. DOPPA only regulates data controllers if they provide services or computer features that are "aimed or designed to reach an audience that is predominantly children".

However, this does not include services or computer features that merely link or link to another service or site directed at children. Data controllers may also be liable under DOPPA if, despite the fact that their services or computer features are not intended for children, they actually know that children are accessing them. In such a case, a data controller may not knowingly use, disclose or compile that child's personal information, nor may it allow another data controller to do the same. A data controller providing services or computer functionality may not advertise or sell content that is not suitable for children. In this regard, DOPPA provides a list of prohibited content, including alcoholic beverages, tobacco, firearms, fireworks, tanning equipment and products, lotteries and gambling, tattoos, drug paraphernalia and pornography. It should be noted that the data controller does not need to track the above if it is using an advertising service and is complying with DOPPA.

### **Legislation of the state of Nevada**

We are posting information here for Nevada residents to provide more information about the law and your privacy rights under Nevada Senate Bill 220 privacy law.

Refusal to sell data. Nevada law allows entities to opt out of the sale of "non-public information" collected through a Website or online service. Under the law, "non-public information" includes:

- first and last name;

physical address, including the street name and the name of the city or town;

email address;

phone number;

social security number;

an identifier that allows you to contact a specific person physically or via the Internet;

any other information about a person collected from him through the Website or online service of the data controller and stored by the data controller in combination with an identifier in a form that makes it possible to identify the person.

Request response time. The data controller has 45 days after receiving a “request from a verified subject”, with a possible extension of 90 days if “reasonably necessary” and subject to notice to the subject. Thus, the response time to the request should not exceed 135 days.

### **Legislation of the Utah state**

We are posting information here for Utah residents to provide more information about the law and your privacy rights under Utah Consumer Privacy Act.

Juvenile policy. In the case of processing personal data concerning a known child (under 13 years), the parent or legal guardian of the known child shall exercise a right on the child's behalf.

Access request. A consumer may exercise a right by submitting a request to a controller, by means prescribed by the controller, specifying the right the consumer intends to exercise. Protection of Persons Under Disability and Their Property, the guardian or the conservator of the consumer shall exercise a right on the consumer's behalf.

Request response time. Controller shall comply with a consumer's request within 45 days after the day on which a controller receives a request to exercise a right, the controller shall:

- take action on the consumer's request; and

inform the consumer of any action taken on the consumer's request.

The controller may extend once the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller. If a controller extends the initial 45-day period, before the initial 45-day period expires, the controller shall:

- inform the consumer of the extension, including the length of the extension; and
- provide the reasons the extension is reasonably necessary.

The 45-day period does not apply if the controller reasonably suspects the consumer's request is fraudulent and the controller is not able to authenticate the request before the 45-day period expires.

The right to non-discrimination. A controller may not discriminate against a consumer for exercising a right by:

- denying a good or service to the consumer;
- charging the consumer a different price or rate for a good or service; or
- providing the consumer a different level of quality of a good or service.

### **Changes and updates**

In case of any changes, we will publish a new version of this Privacy Notice on our App.

If there are significant changes that affect your privacy, we will notify you by email or display information on the App and ask for your consent (if necessary).