IPOSTAL1 - GLOBAL PRIVACY POLICY

This Privacy Policy is in effect as of January 1, 2020.
Last updated: January 1, 2019

We at iPostal1 (defined below) respect and protect the privacy of visitors to our websites and our customers. This Privacy Policy describes our information handling practices when you access our services, which include our websites located at ipostal1.com, iworkspacemail.com, and/or any other websites, pages, features, or content we own or operate (collectively, the "**Site**(**s**)"), or when you use the iPostal1 mobile app and/or any other mobile apps we own or operate, any iPostal1 API or third party applications relying on such an API, and related services (referred to collectively hereinafter as "**Services**").

Please take a moment to read this Privacy Policy carefully. If you have any questions about this Policy, please submit your request via our global privacy team at dataprotection@uszoom.com.

ACCEPTANCE OF THIS PRIVACY POLICY

By accessing and using our Services, you signify acceptance to the terms of this Privacy Policy. Where we require your consent to process your personal information, we will ask for your consent to the collection, use, and disclosure of your personal information as described further below. We may provide additional periodical disclosures or information about the data processing practices of specific Services. These notices may supplement or clarify our privacy practices or may provide you with additional choices about how we process your data.

If you do not agree with *or* you are not comfortable with any aspect of this Privacy Policy, you should immediately discontinue access or use of our Services.

CHANGES TO THIS PRIVACY POLICY

We may modify this Privacy Policy from time to time which will be indicated by changing the date at the top of this page. If we make any material changes, we may notify you by email (sent to the email address specified in your account), by means of a notice on our

Services, or Sites, prior to the change becoming effective, or as otherwise required by law.

OUR RELATIONSHIP TO YOU

iPostal1 (collectively "**USZoom**", "**iP1**", "**we**", "**us**" and "**our**"), currently operates entities in the USA in order to provide Services to our customers. The following table describes which entity you are contracting with:

Where You Reside	Services Provided	Operating Entity	Contact Address
The United States, Europe, or anywhere else worldwide	Digital Mailbox Virtual Office	USZoom LLC	400 Rella Blvd, Suite 123, Montebello NY 10901 USA

You may be asked to provide personal information anytime you are in contact with iP1. The iP1 corporate family of companies may share your personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, and content (additional details below). For example, even if you do not reside in the United States (the "**US**"), your information may be shared with the appropriate company within the USZoom LLC corporate family which provides global support for all Services including technical infrastructure, product development, security, compliance, fraud prevention, and customer support.

If you have any questions about your iP1 Account, your personal information, or this Privacy Policy, please submit your request to service@ipostal1.com or dataprotection@uszoom.com, respectively.

THE PERSONAL INFORMATION WE COLLECT

Personal information is data that identifies an individual or relates to an identifiable individual. This includes information you provide to us, information which is collected about you automatically, and information we obtain from third parties.

Information you provide to us

To establish an account and access our Services, we'll ask you to provide us with some important information about you. This information is either required by law (e.g. to verify your identity), necessary to provide the requested services (e.g. you will need to provide your bank account number if you'd like iP1 to perform check deposit services), or is relevant for certain specified purposes, described in greater detail below. As we add new features and Services, you may be asked to provide additional information.

Please be advised that we may not be able to serve you as effectively or offer you our Services if you choose not to share certain information with us. Any information you provide to us that is not required is voluntary.

We may collect the following types of information from you:

- **Personal Identification Information**: Full name, date of birth, nationality, gender, signature, utility bills, photographs, phone number, home and email addresses.
- **Formal Identification Information**: Government issued identity document such as Passport, Driver's License, National Identity Card, State ID Card, Tax ID number, passport number, driver's license details, national identity card details, visa information, and/or any other information deemed necessary to comply with our legal obligations under postal, financial, export or anti-money laundering laws and regulations.
- **Institutional Information**: Employer Identification number (or comparable number issued by a government), proof of legal formation (e.g. Articles of Incorporation), personal identification information for all material beneficial owners.
- **Financial Information**: Bank account information, payment card primary account number (PAN), transaction history, and/or tax identification.

- **Transaction Information**: Information about the transactions you make on our Services, such as the name and address of the recipient (in case of mail forwarding).
- **Employment Information**: Office location, job title, and/or description of role.
- **Correspondence**: Survey responses, information provided to our support team or user research team.

Information we collect from you automatically

We receive and store certain types of information automatically, such as whenever you interact with the Sites or use the Services. This information helps us address customer support issues, improve the performance of our Sites and applications, provide you with a streamlined and personalized experience, and protect your account from fraud by detecting unauthorized access. Information collected automatically includes:

- **Online Identifiers**: Geo location/tracking details, browser fingerprint, operating system, browser name and version, and/or personal IP addresses.
- **Usage Data**: Authentication data, security questions, click-stream data, and other session data collected via cookies and similar technologies.

For example, we may automatically receive and record the following information on our server logs:

- How you came to and use the Services (from our adverts and affiliate links);
- Device type and unique device identification numbers;
- Device event information (such as crashes, system activity and hardware settings, browser type, browser language, the date and time of your request and referral URL);
- How your device interacts with our Sites and Services, including pages accessed and links clicked;
- Broad geographic location (e.g. country or city-level location); and
- Other technical data collected through cookies, and other similar technologies that uniquely identify your session.

We may also use identifiers to recognize you when you access our Sites via an external link, such as a link appearing on a third-party site.

HOW WE PROTECT AND STORE PERSONAL INFORMATION

We understand how important your privacy is, which is why iP1 maintains (and requires subcontractors and third parties it shares your information with to maintain) appropriate physical, technical and administrative safeguards to protect the security and confidentiality of the personal information you entrust contractually to us.

We may store and process all or part of your personal and transactional information, including certain payment information, such as your encrypted bank account and/or routing numbers, in the US and elsewhere in the world where our facilities or our service providers are located. We protect your personal information by maintaining physical, electronic, and procedural safeguards in compliance with the applicable laws and regulations.

For example, we use computer safeguards such as firewalls and data encryption, we enforce physical access controls to our buildings and files, and we authorize access to personal information only for those employees who require it to fulfil their job responsibilities. Full credit card data is securely transferred and hosted off-site by payment vendors like First Data, and PayPal in compliance with Payment Card Industry Data Security Standards (PCI DSS). This information is not accessible to iP1 or iP1 staff. For more information about how First Data stores and uses your information, please see their Privacy Policy at https://www.firstdata.com/en_us/privacy/binding-corporate-rules.html

However, we cannot guarantee that loss, misuse, unauthorized acquisition, or alteration of your data will not occur. Please recognize that you play a vital role in protecting your own personal information. When registering with our Services, it is important to choose a password of sufficient length and complexity, to not reveal this password to any third-party, and to immediately notify us if you become aware of any unauthorized access to or use of your account.

Furthermore, we cannot ensure or warrant the security or confidentiality of information you transmit to us or receive from us by Internet or wireless connection, including email, phone, or SMS, since we have no way of protecting that information once it leaves and

until it reaches us. If you have reason to believe that your data is no longer secure, please contact us using the contact information provided in this Privacy Policy.

RETENTION OF PERSONAL INFORMATION

We store your personal information securely throughout the life of your iP1 Account. We will only retain your personal information for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting obligations or to resolve disputes. While retention requirements vary by jurisdiction, information about our typical retention periods for different aspects of your personal information are described below.

- Personal information collected to comply with our legal obligations under postal, financial, export, or anti-money laundering laws may be retained after account closure for as long as required under such laws.
- Contact Information such as your name, email address and telephone number on an ongoing basis until you unsubscribe and retain such records for a reasonable time thereafter.
- Recording of our telephone calls with you may be kept for a reasonable time period.
- Information collected via technical means such as cookies, webpage counters and other analytics tools is kept for a reasonable period of time.

CHILDREN'S PERSONAL INFORMATION

We do not knowingly collect personal data from users deemed to be children under their respective national laws. As different countries may derogate from the GDPR standards and legislate their own age restrictions, iP1 will require parental consent when required to do so by the local law of the country from where the signup originates.

If a user submitting personal information is suspected of being a legal minor and is unable to satisfy the parental consent requirement, iP1 will require such user to close his or her account and will not allow the user to continue using our Services. iP1 will also

take steps to delete the information as soon as possible. Please notify us if you know of any underage individuals using our Services so we can take action to prevent access to our Services.

INFORMATION COLLECTED FROM THIRD PARTIES

From time to time, we may obtain information about you from third party sources as required or permitted by applicable law. These sources may include:

- **Public Databases, Credit Bureaus & ID Verification Partners**: We obtain information about you from ID verification partners for purposes of verifying your identity in accordance with applicable law. ID verification partners like World-Check use a combination of government records and publicly available information about you to verify your identity. Such information may include your name, address, job role, public employment profile, credit history, status on any sanctions lists maintained by public authorities, and other relevant data. We obtain such information to comply with our legal obligations, such as postal, financial, export, and anti-money laundering laws. In some cases, we may process additional data about you to ensure our Services are not used fraudulently or for other illicit activities. In such instances, processing is necessary for us to continue to perform our contractual obligations with you and others. World-Check's Privacy Policy, available at https://www.refinitiv.com/en/products/world-check-kyc-screening/privacy-statement/, describes its collection and use of personal data.
- **Joint Marketing Partners & Resellers**: For example, unless prohibited by applicable law, joint marketing partners or resellers may share information about you with us so that we can better understand which services may be of interest to you.
- **Advertising Networks & Analytics Providers**: We work with these providers to provide us with de-identified information about how you found our Sites and how you interact with the Sites and Services. This information may be collected prior to account creation.

ANONYMIZED AND AGGREGATED DATA

Anonymization is a data processing technique that removes or modifies personal information so that it cannot be associated with a specific individual. Except for this section, none of the other provisions of this Privacy Policy applies to anonymized or aggregated customer data (i.e. information about our customers that we combine together so that it no longer identifies or references an individual customer).

We may use anonymized or aggregate customer data for any business purpose, including to better understand customer needs and behaviours, improve our products and services, conduct business intelligence and marketing, and detect security threats. We may perform our own analytics on anonymized data or enable analytics provided by third parties.

Types of data we may anonymize include, transaction data, click-stream data, performance metrics, and fraud indicators.

HOW YOUR PERSONAL INFORMATION IS USED

Our primary purpose in collecting personal information is to provide you with a secure, smooth, efficient, and customized experience. We generally use personal information to create, develop, operate, deliver, and improve our Services, content and advertising; and for loss prevention and anti-fraud purposes.

We may use this information in the following ways:

1) **To maintain legal and regulatory compliance**

Most of our core Services are subject to laws and regulations requiring us to collect, use, and store your personal information in certain ways. For example, iP1 must identify and verify customers using our Services in order to comply with postal, financial, export, and anti-money laundering laws across jurisdictions. This includes collection of a signed and notarized form PS 1583 and storage of your photo identification. In addition, we use

third parties to verify your identity by comparing the personal information you provide against third-party databases and public records.

2) **To enforce our terms in our user agreement and other agreements**

iP1 handles sensitive information, such as your scanned mail, identification and financial data, so it is very important for us and our customers that we actively monitor, investigate, prevent, and mitigate any potentially prohibited or illegal activities, enforce our agreements with third parties, and/or prevent and detect violations of our posted user agreement or agreements for other Services. In addition, we need to collect fees based on your use of our Services. We collect information about your account usage and closely monitor your interactions with our Services. We may use any of your personal information collected for these purposes. The consequences of not processing your personal information for such purposes is the termination of your account.

3) **To detect and prevent fraud and/or funds loss**

We process your personal information in order to help detect, prevent, and mitigate fraud and abuse of our Services and to protect you against account compromise or funds loss.

4) **To provide iP1's Services**

We process your personal information to provide the Services to you. For example, when you want to deposit checks on our platform, we require certain information such as the essential payment information. We cannot provide you with Services without such information.

5) **To provide Service communications**

We send administrative or account-related information to you to keep you updated about our Services, inform you of relevant security issues or updates, or provide other transaction-related information. Without such communications, you may not be aware of important developments relating to your account that may affect how you can use our Services. You may not opt-out of receiving critical service communications, such as emails or mobile notifications sent for legal or security purposes.

6) **To provide customer service**

We process your personal information when you contact us to resolve any questions, disputes, collect fees, or to troubleshoot problems. Without processing your personal information for such purposes, we cannot respond to your requests and ensure your uninterrupted use of the Services.

7) **To ensure quality control**

We process your personal information for quality control and staff training to make sure we continue to provide you with accurate information. If we do not process personal information for quality control purposes, you may experience issues on the Services such as inaccurate transaction records or other interruptions.

8) **To ensure network and information security**

We process your personal information in order to enhance security, monitor and verify identity or service access, combat spam or other malware or security risks and to comply with applicable security laws and regulations. The threat landscape on the internet is constantly evolving, which makes it more important than ever that we have accurate and up-to-date information about your use of our Services. Without processing your personal information, we may not be able to ensure the security of our Services.

9) **For research and development purposes**

We process your personal information to better understand the way you use and interact with iP1's Services. In addition, we use such information to customise, measure, and improve iP1's Services and the content and layout of our website and applications, and to develop new services. Without such processing, we cannot ensure your continued enjoyment of our Services.

10) **To facilitate corporate acquisitions, mergers, or transactions**

We may process any information regarding your account and use of our Services as is necessary in the context of corporate acquisitions, mergers, or other corporate transactions. You have the option of closing your account if you do not wish to have your personal information processed for such purposes.

11) **To engage in marketing activities**

Based on your communication preferences, we may send you marketing communications (e.g. emails or mobile notifications) to provide you with promotional offers. Our marketing will be conducted in accordance with your advertising marketing preferences and as permitted by applicable law.

12) **Consent based usage**

Excluding any contrary undertaking hereunder regarding your personal information, any disclosure of your personal information is subject to your consent.

We will not use your personal information for purposes other than those purposes we have disclosed to you, without your permission. From time to time, and as required under the applicable law, we may request your permission to allow us to share your personal information with third parties. You may opt out of having your personal information shared with third parties or allowing us to use your personal information for any purpose that is incompatible with the purposes for which we originally collected it or subsequently obtained your authorization. If you choose to so limit the use of your personal information, certain features or iP1's Services may not be available to you.

EEA Data Subjects

iP1 determines the means and purposes of processing your personal information in relation to the Services provided to you (in the EU General Data Protection Regulation ("**GDPR**"), the entity performing such function is referred to as a "**Data Controller**").

Commercial Mail Receiving Agent ("CMRA" or "Shipping Stores") listed on our platform, act on our behalf and do not control the means and purpose of the processing, (in the GDPR, the entity performing such function is referred to as a "**Data Processor**").

However, should you elect to opt in to receive advertising or marketing material from a CMRA/Shipping Store that provides services on our platform, this will legally define them per GDPR as Controllers of the personal data you have chosen to share with them. In the foregoing instances, iP1 shall not be classified as a Data Controller, Joint Data Controller, or Processor with regards to the personal data shared with the CMRA/Shipping Store.

Legal Bases for Processing your Information

For individuals who are located in the European Economic Area, United Kingdom or Switzerland (collectively "**EEA Residents**") at the time their personal data is collected, we rely on legal bases for processing your information under Article 6 of the GDPR. We generally only process your data where we are legally required to, where processing is necessary to perform any contracts we entered with you (or to take steps at your request prior to entering into a contract with you), for our legitimate interests to operate our business or to protect IP1's or your, property, rights, or safety, or where we have obtained your consent to do so. Below is a list of the purposes described in our policy with the corresponding legal bases for processing.

Section & Purpose of Processing	**Legal Bases for Processing**
2) To enforce our terms in our user agreement and other agreements 4) To provide IP1's Services 5) To provide Service communications 6) To provide customer service 7) To ensure quality control	Based on our contract with you or to take steps at your request prior to entering into a contract.
(9) For research and development purposes (10) To enhance your experience (11) To facilitate corporate acquisitions, mergers, or transactions (12) To engage in direct marketing activities	Based on our legitimate interests. When we process your personal data for our legitimate interests, we always ensure that we consider and balance any potential impact on you and your rights under data protection laws.
(1) To maintain legal and regulatory compliance	Based on our legal obligations, obligations, the public interest, or in your

Section & Purpose of Processing	**Legal Bases for Processing**
(3) To detect and prevent fraud and/or funds loss (8) To ensure network and information security	vital interests.
(11) To engage in third party marketing activities (12) Consent based usage	Based on your consent.

Marketing

Direct Marketing: Direct marketing includes any communications to you that are only based on advertising or promoting our products and services. We will only contact you by electronic means (email or SMS) based on our legitimate interests, as permitted by applicable law, or your consent. To the extent we can rely on legitimate interest under the applicable law, we will only send you information about our Services that are similar to those which were the subject of a previous sale or negotiations of a sale to you. If you are a new customer, we will contact you by electronic means for marketing purposes only if you have consented to such communication. If you do not want us to send you marketing communications, please go to your account settings to opt-out or submit a request to service@iPostal1.com. You may raise such objection with regard to initial or further processing for purposes of direct marketing, at any time and free of charge. Direct marketing includes any communications to you that are only based on advertising or promoting our products and services.

Third Party Marketing: We will not share your personal information to any third parties for marketing purposes.

WHY WE SHARE PERSONAL INFORMATION WITH OTHER PARTIES

We take care to allow your personal information to be accessed only by those who require access to perform their tasks and duties, and to share only with third parties who have a legitimate purpose for accessing it. **IP1 will never sell or rent your personal information to third parties without your explicit consent**. We will only share your information in the following circumstances:

- With third party identity verification services in order to prevent fraud. This allows IP1 to confirm your identity by comparing the information you provide us to public records and other third-party databases. These service providers may create derivative data based on your personal information that can be used solely in connection with the provision of identity verification and fraud prevention services. For example:
  - We may use Notarize Inc. or similar services (to verify your identity by video session. The information collected from your photo may include biometric data. Notarize Inc's Privacy Policy, available at https://www.notarize.com/privacy, describes its collection and use of personal data.
  - We may use MAXMind, Inc. to detect and prevent fraudulent activity on your account in real time. Information shared with MAXMind is treated in accordance with its Privacy Policy, available at https://www.maxmind.com/en/privacy-policy.
- With financial institutions with which we partner to process payments you have authorized.
- With CMRA's and other service providers under contract who help with parts of our business operations. Our contracts require these service providers to only use your information in connection with the services they perform for us and prohibit them from selling your information to anyone else. Examples of the types of service providers we may share personal information with (other than those mentioned above) include:
  - Payment processing
  - Customer support
- With companies or other entities that we plan to merge with or be acquired by. You will receive prior notice of any change in applicable policies.

- With companies or other entities that purchase IP1 assets pursuant to a court-approved sale or where we are required to share your information pursuant to insolvency law in any applicable jurisdiction.
- With our professional advisors who provide banking, legal, compliance, insurance, accounting, or other consulting services in order to complete third party financial, technical, compliance and legal audits of our operations or otherwise comply with our legal obligations.
- With law enforcement, officials, or other third parties when we are compelled to do so by a subpoena, court order, or similar legal procedure, or when we believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity, or to investigate violations of our user agreement or any other applicable policies.

HOW WE PROTECT AND STORE PERSONAL INFORMATION

We understand how important your privacy is, which is why IP1 maintains (and contractually requires third parties it shares your information with to maintain) appropriate physical, technical and administrative safeguards to protect the security and confidentiality of the personal information you entrust to us.

We may store and process all or part of your personal and transactional information, including certain payment information, such as your encrypted bank account in the US and elsewhere in the world. We protect your personal information by maintaining physical, electronic, and procedural safeguards in compliance with the applicable laws and regulations.

For example, we use computer safeguards such as firewalls and data encryption, we enforce physical access controls to our buildings and files, and we authorize access to personal information only for those employees who require it to fulfil their job responsibilities. Full credit card data is securely transferred and hosted off-site by payment vendors like First Data, PayPal, or Worldpay, (UK) Limited, Worldpay Limited, or Worldpay AP Limited (collectively "Worldpay") in compliance with Payment Card Industry Data Security Standards (PCI DSS). This information is not accessible to IP1 or IP1 staff.

For more information about how Worldpay stores and uses your information, please see Worldpay's Privacy Policy at https://www.worldpay.com/uk/worldpay-privacy-notice.

However, we cannot guarantee that loss, misuse, unauthorized acquisition, or alteration of your data will not occur. Please recognize that you play a vital role in protecting your own personal information. When registering with our Services, it is important to choose a password of sufficient length and complexity, to not reveal this password to any third parties, and to immediately notify us if you become aware of any unauthorized access to or use of your account.

Furthermore, we cannot ensure or warrant the security or confidentiality of information you transmit to us or receive from us by Internet or wireless connection, including email, phone, or SMS, since we have no way of protecting that information once it leaves and until it reaches us. If you have reason to believe that your data is no longer secure, please contact us using the contact information provided in this Privacy Policy.

RETENTION OF PERSONAL INFORMATION

We store your personal information securely throughout the life of your iP1 Account. We will only retain your personal information for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting obligations or to resolve disputes. While retention requirements vary by jurisdiction, information about our typical retention periods for different aspects of your personal information are described below.

- Personal information collected to comply with our legal obligations under postal, financial, export, or anti-money laundering laws may be retained after account closure for as long as required under such laws.
- Contact Information such as your name, email address and telephone number on an ongoing basis until you unsubscribe and retain such records for a reasonable time thereafter.
- Recording of our telephone calls with you may be kept for a reasonable time period.
- Information collected via technical means such as cookies, webpage counters and other analytics tools is kept for a reasonable period of time.

CHILDREN'S PERSONAL INFORMATION

We do not knowingly collect personal data from users deemed to be children under their respective national laws. As different countries may derogate from the GDPR standards and legislate their own age restrictions, iP1 will require parental consent when required to do so by the local law of the country from where the signup originates.

If a user submitting personal information is suspected of being a legal minor and is unable to satisfy the parental consent requirement, iP1 will require such user to close his or her account and will not allow the user to continue using our Services. iP1 will also take steps to delete the information as soon as possible. Please notify us if you know of any underage individuals using our Services so we can take action to prevent access to our Services.

YOUR PRIVACY RIGHTS

Depending on applicable law where you reside, you may be able to assert certain rights related to your personal information identified below. If any of the rights listed below are not provided under law for your operating entity or jurisdiction, IP1 has absolute discretion in providing you with those rights.

Your rights to personal information are not absolute. Depending upon the applicable law, access may be denied: (a) when denial of access is required or authorized by law; (b) when granting access would have a negative impact on another's privacy; (c) to protect our rights and properties; (d) where the request is frivolous or vexatious, or for other reasons.

- **Access and portability**. You may request that we provide you a copy of your personal information held by us. This information will be provided without undue delay subject to a potential fee associated with gathering of the information (as

permitted by law), unless such provision adversely affects the rights and freedoms of others. In certain circumstances, you may request to receive your personal information in a structured, commonly used and machine-readable format, and to have us transfer your personal information directly to another data controller.

- **Rectification of incomplete or inaccurate personal information**. You may rectify or request us to rectify or update any of your personal information held by IP1 that is inaccurate. You may do this at any time by logging in to your account or informing at service@ipostal1.com.
- **Erasure**. You may request to erase your personal information, subject to applicable law. If you close your IP1 Account, we will mark your account in our database as "Closed," but will keep certain account information, including your request to erase, in our database for a period of time as described above. This is necessary to deter fraud, by ensuring that persons who try to commit fraud will not be able to avoid detection simply by closing their account and opening a new account, and to comply with IP1's legal obligations. However, if you close your account, your personal information will not be used by us for any further purposes, nor shared with third parties, except as necessary to prevent fraud and assist law enforcement, as required by law, or in accordance with this Privacy Policy.
- **Withdraw consent**. To the extent the processing of your personal information is based on your consent, you may withdraw your consent at any time. Your withdrawal will not affect the lawfulness of IP1's processing based on consent before your withdrawal.
- **Restriction of processing**. In some jurisdictions, applicable law may give you the right to restrict or object to us processing your personal information under certain circumstances. We may continue to process your personal information if it is necessary for the defence of legal claims, or for any other exceptions permitted by applicable law.
- **Automated individual decision-making, including profiling**. IP1 relies on automated tools to help determine whether a transaction or a customer account presents a fraud or legal risk. In some jurisdictions, you have the right not to be subject to a decision based solely on automated processing of your personal information, including profiling, which produces legal or similarly significant effects on you, save for the exceptions applicable under relevant data protection laws.

How to make a privacy request

You can make privacy rights requests relating to your personal information by contacting us via dataprotection@uszoom.com.

How to lodge a complaint

If you believe that we have infringed your rights, we encourage you to first submit a request via dataprotection@uszoom.com so that we can try to resolve the issue or dispute informally. If that does not resolve your issue, you may contact the IP1 Data Protection Manager at shlomof@uszoom.com.

CALIFORNIA PRIVACY RIGHTS

In addition to the rights provided for above, if you are a California resident, you have the right to request information from us regarding whether we share certain categories of your personal information with third parties for the third parties' direct marketing purposes. To the extent we share your personal information in this way, you may receive the following information:

- (a) the categories of information we disclosed to third parties for the third parties' direct marketing purposes during the preceding calendar year; and
- (b) the names and addresses of third parties that received such information, or if the nature of their business cannot be determined from the name, then examples of the products or services marketed.

Effective January 1, 2020, pursuant to the California Consumer Privacy Act of 2018 ("CCPA"), California residents have certain rights in relation to their personal information, subject to limited exceptions. Any terms defined in the CCPA have the same meaning when used in this California Privacy Rights section.

- For personal information collected by us during the preceding 12 months that is not otherwise subject to an exception, California residents have the right to access and delete their personal information. IP1 will not discriminate against those who exercise their rights. Specifically, if you exercise your rights, we will not deny you services, charge you different prices for services or provide you a different level or quality of services.
- To the extent we sell your personal information to third parties, you also have the right to request that we disclose to you: (i) the categories of your personal information that we sold, and (ii) the categories of third parties to whom your personal information was sold. You have the right to direct us not to sell your personal information.
- **IP1 does not sell your personal information in its ordinary course of business and will never sell your personal information to third parties without your explicit consent**.

- Should IP1 engage in any of the activities listed in this section, your ability to exercise these rights will be made available to you in your account settings. You can exercise your rights by contacting us via our dataprotection@uszoom.com so that we may consider your request.

If you are a California resident, you may designate an authorized agent to make a request to access or a request to delete on your behalf. We will respond to your authorized agent's request if they submit proof that they are registered with the California Secretary of State to be able to act on your behalf or submit evidence you have provided them with power of attorney pursuant to California Probate Code section 4000 to 4465. We may deny requests from authorized agents who do not submit proof that they have been authorized by you to act on their behalf or are unable to verify their identity.

HOW TO CONTACT US

If you have questions or concerns regarding this Privacy Policy, or if you have a complaint, please contact us at dataprotection@uszoom.com, or by writing to us at the address of your operating entity (provided above).