IT Eagle Eye

Privacy Policy

Scope

This Privacy Policy applies to the information we collect though our mobile apps, websites, via phone calls, emails, and other service related contact between IT Eagle Eye and the Customer. This privacy notice does not apply to information we collect through other methods or sources, including sites owned or operated by our affiliates, vendors, or partners.

HOW DO WE COLLECT PERSONAL DATA?

We collect Personal Data in four ways: direct entry or provision by the Customer, automated third party collections, non-automated collection from third party services or individuals, and internal business operations. We collect Personal Data from our Customers, their authorized employees or contractors, and from our own employees, contractors, or applicants. When requested Personal Data is not provided, it may inhibit or cease our ability to provide the services that requires the requested Personal Data. We may use the following sources to collect Personal Data:

- You (Direct) – We collect information from you directly via online forms, applications, business correspondence.
- You (Automated) – We collect technical information, including session details from the device that you use to access our websites, applications and other internet based interactions. More information on this collection is available in the Website and Cookies section of this Privacy Policy.
- Employees – We collect Personal Data to ensure the qualification and integrity of our employees and contractors in order to protect our services and handling of Personal Data.

- Clients – We collect transaction/financial data related to payment transactions that you initiate with us.
- Identity Protection Services – We collect data to ensure adequate fraud protection for payment transactions.
- Referral Partners – We collect data from referral partners who have directed you to our company.
- Third Party Servicers – We may also receive data from providers we use in providing services. These include, but are not limited to, Merchant Account Servicers, Fraud Prevention Servicers, Government/Law Enforcement, Data Aggregators, and Other Vendors.
- Public Record – We collect information about business registrations and filings, business standing, business marketing practices, business financial solvency, public postings, reviews, or comments, and other related information.
- Internal – We collect and create Personal Data by keeping records of correspondence and use of our services.

WHAT PERSONAL DATA DO WE COLLECT?

We collect and process the Personal Data described below under each method of collection.

DIRECT PROVISION

Any Personal Data you provide to us directly or indirectly through a third party, including employment agencies, merchants, or other vendors who use our products.

- Correspondence and Verification Data (including name, email, phone number, biometrics, location, job title)
- Form Data (Information provided by entering into a form, rather directly or indirectly through provision to our agents, partners, resellers, third party servicers, or direct agents.)

- Financial Data (including Bank Accounts, Bankruptcy History, and Payment Details)
- Business Data (Information concerning ownership, industry designation, and other pertinent data provided in order to contract with us.)

Automated Collections

When using our website, mobile app, or services, some information may be collected automatically to facilitate provision and protection of those services. This data includes:

- Public Sources (e.g. Company Registries and Company Filings)
- Transactional Data and Related Information
- Website or Mobile App Access and Use Data

Third Party Collections (Non-Automated)

- Public Listings
- Internet Search Engines
- Websites or Affiliate Websites
- Ads or Marketing Material
- Public Reviews or Complaints
- Trade References

Business Operations

We access, create, store, and transfer Personal Data when collecting technical data or usage date, including transactional data. We also access, create, store, and transfer Personal Data during normal business operations. Data collected in these manners includes:

- IP Address

- Browser and Operating System Details
- Access Records or Login Data
- Transactional Data
- Correspondence (Phone records, emails, fax, and other requests and responses)
- Internal Operational Reports
- External Reports (Created for third parties as required by law)

HOW DO WE USE YOUR PERSONAL DATA?

We use Personal Data for internal use only. This means we use or access your Personal Data only to provide services, process requests, support operations, perform fraud checks, and as required by law. We only provide information to third parties in conjunction with the performance of these duties or legal requests. The services we provide that utilize Personal Data include:

- Business Administration and Operations (e.g. Updating Records)
- Provision of Contracted Services
- Fraud Prevention Checks / Risk Management
- Internal Research and Development
- Legal Requirement Fulfillment
- Direct Marketing Communications
- Relationship Management and Support
- Payment Transactions

DATA SHARING AND LIMITATIONS

We share Personal Data with our Authorized Affiliates and with Third Party Providers in order to provide, enhance, and monitor services to our Customers. We do not share any Personal Data for marketing purposes unless we are authorized by the Customer. Information collected on this site is not sold or transferred to any person or party that is not directly involved in normal business operations. Your Personal Data is only shared to provide the services detailed in this privacy statement and to comply with legal or regulatory requirements. The following list denotes where your Personal Data may be shared:

- Our Service Providers
- Credit Reference Agencies
- Fraud Protection Services
- Identity Verification Agencies
- Payment Facilitators/Transaction Networks
- Auditors and Other Professional Advisers
- Legal Advisers
- Third Parties for Review for Sell or Transfer of all or a portion of our Business
- Sub-Contractors for Our Vendors
- Tax Authorities
- Any Third Party Where Required By Law

LIMIT SHARING

We only share data as required to perform our services and comply with legal requirements. Optional or non-required personal data sharing will only occur with an express opt-in choice by the customer.

Legal Requests

In certain situations we may be required to disclose personal data in response to lawful request by public authorities, including to meet national security or law enforcement requirements.

DATA HANDLING

Security Measures

IT Eagle Eye takes appropriate technical and organizational security measures to provide protection against unauthorized access, unlawful destruction, loss, alteration, and unauthorized disclosure of Personal Data. Security measures are implemented and maintained in accordance with ISO 27001 standards. This compliance is reviewed and verified annually.

Non-Discrimination

Personal Data that is provided by you or collected automatically, may be used to make automated decisions and limit our provision of services. When automated decisions occur, they are due to data collected in regards to credit scoring, fraud prevention, legal restrictions, or restrictions imposed to mitigate fraud and liability by our partners.

Automated and non-automated decisions are only made on the basis of non-discriminatory information that has been made available to us and that has been verified against minimum contractual or legal requirements, when required by law.

We regularly review our decision processes to ensure that they remain unbiased and effective

International Transfer

Personal Data is transferred outside of the European Economic Area when it is collected and shared with our Transaction Network. International transfers are done in accordance with our sharing and privacy policy.

When we transfer your data internationally, we require all authorized affiliates to commit to the same level of privacy protection as outlined in this privacy policy. We also ensure that your data is only transferred in accordance with the following guidelines:

- Encryption of data to prevent an unauthorized access or use during data transmission.
- Contracts with third parties require them to attest to equivalent protections for Personal Data handling.
- Data is transferred only for the use purposes described in our privacy policy.

Accountability

IT Eagle Eye's accountability for personal data that it receives in the United States under the Data Privacy Frameworks and subsequently transfers to a third party is described in the Data Privacy Framework Principles. In particular, IT Eagle Eye remains responsible and liable under the Data Privacy Framework Principles if third-party agents that it engages to process personal data on its behalf do so in a manner inconsistent with the Principles, unless IT Eagle Eye proves that it is not responsible for the event giving rise to the damage.

Deletion and Retention

We store your Personal Data for the length of time required based on the reasons that it was collected. This includes data collected to provide services, support business operations, and as required to meet legal, accounting, regulatory or reporting requirements. This includes retaining Personal Data for the length of any contracted service terms with IT Eagle Eye or authorized affiliates and as required by law.

Following the conclusion of our use or need for the Personal Data, we retain sensitive Personal Data for eighteen months to safeguard against further need for one of the use cases described in this policy. Personal Data that has been de-identified may be kept beyond this period.

Questions concerning our retention of your Personal Data should be addressed to our designated Data Protection Officer via the contact method provided in this Privacy Policy.

Notification

When there are significant changes to our treatment of your Personal Data and changes to this Privacy Policy, we will notify you in advance of those changes being implemented. This policy is posted publicly and kept up to date on our website at https://iteagleeye.com/legal/privacy-policy/.

WEBSITE AND COOKIES

Our website is not directed to children or teens under the age of majority. IT Eagle Eye does not knowingly collect Personal Data at our website from persons who are not legal adults.

Cookies

We may employ the use of cookies or web beacons in your interactions with our website(s) or mobile applications. Cookies and web beacons are text files and tags respectively, which may be used to send information to our web server. This information may be used to help understand interaction with our website, improve suggestions to you, apply remembered choices, such as log in, and analytics. We may employ the use of third party analytics companies or software to help process this data. More information on our use of cookies is available at https://iteagleeye.com/legal/cookie-policy/.

Third Party Websites

We may link or refer to other websites for our affiliated companies. When those websites have their own privacy notices, this privacy notice does not apply. Refer to the privacy notice that is directly posted by those companies for information governing use of their website and services.

Our website may also contain links or other referrals to third-party websites. IT Eagle Eye is not responsible for the privacy practices of any third party, and this privacy notice does not apply to their websites. IT Eagle Eye does not guarantee, approve, or endorse any information, material, services, or products contained on or available through any linked or referenced third-party website. IT Eagle Eye provides links and referrals to third-party websites as a convenience and visiting or using linked third-party websites is at your own risk.

Acceptance

By using our website or services, you certify that you are of legal adult age and agree with the terms of this Privacy Policy. You grant permission for us to collect the Personal Data detailed in this policy and certify understanding of your rights concerning your Personal Data.

INDIVIDUAL RIGHTS

We respond to all requests to exercise individual rights concerning Personal Data in a timely manner. When your requests are numerous, complex or require additional processing times, we may require greater than thirty days from the time or receipt of the request. In these instances, you will be notified in writing of the time delay.

Consent

Use of our website or services directly or through our Clients constitutes acceptance and consent to have your Personal Data collected and used in accordance with this privacy policy. That consent may be withdrawn at any time, but we may not be able to continue to provide you with the requested service in these cases.

Objections to Processing

If you believe that our processing of your Personal Data impacts your fundamental rights and freedoms, then you also have the right to object to our processing, where we may have processed information incorrectly or unlawfully. This objection can be made by directly contacting our Data Protection Officer. Complaints that cannot be

satisfactorily handled by direct contact to the designated Data Protection officer, may be submitted to an independent dispute resolution mechanism as described in this Privacy Policy.

Access to Personal Data

You are entitled to know if we are processing your Personal Data, the reason for that processing, and the contents of the collected Personal Data, as well as other information about our processing activities. Questions about Personal Data that we have accessed may be directed to our Data Protection Officer.

When reasonably possible, we will provide to you or an authorized third party, an accounting of the Personal Data that we have on file. This accounting will be in a structured, machine readable format. The accounting will include Personal Data that has been provided to us directly by you. This does not include internal algorithms or intellectual property including reports that were created during our normal business operations, or information gathered from outside sources except where it may be used to perform automated decisions concerning your account.

In the event that we are not able to provide the information you requested, we will provide you with a written explanation for our decision. For example, we are not required to comply with a request to erase data if processing the data is necessary to: exercise freedom of expression and information; comply with law or legal claims; act in the interest of the public health or public interest; or support scientific or historical research purposes or statistical purposes.

Data Restrictions

You may restrict how we use your Personal Data by limiting what Personal Data you allow to be collected or by limiting our use of previously collected Personal Data. In these cases, you understand that limitation may impede our ability to provide you with services.

We will provide an individual opt-out choice, or opt-in for sensitive data, before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To

request to limit the use and disclosure of your personal information, please submit a written request to compliance@iteagleeye.com

You may restrict the use of automated decisions based on your data, except as required to enter into contracts with us, as approved by law, or where we have you consented to automated decisions. When automated decisions do occur, you have the right to appeal those decisions and obtain human intervention to contest the result of the objected automated decision, except where the automated decision is accepted by law.

Data Integrity

When you believe that Personal Data collected is incorrect, you have the right to correct the Personal Data in question. Corrections must be verified in both the source and the accuracy of the provided Personal Data in order for us to update this information. Verification of you to access or correct your Personal Data may require you to divulge additional Personal Data for authorization purposes.

Erasure of Personal Data

You have the right to request deletion of Personal Data that we have collected when there is not a reason for us to continue processing it and you have successfully exercised your right to object to processing of Personal Data. You may also request deletion or erasure of Personal Data in accordance with legal requirements.

Limitations

These rights may be limited for legal or other valid reasons that inhibit us from providing the requested access or service in regards to your Personal Data. When that is the case, we are not obliged to fulfill a request to exercise these rights. In those instances, you will be informed of the limitation to our ability to respond to your request and the reason that the request is not able to be filled.

We reserve the right to charge a fee for these services when the request is clearly unfounded, repetitive, or excessive. We also reserve the right to refuse to comply with your request in these circumstances. We have the right to contact you concerning your

request and to gather information concerning your request and the reason for your request prior to fulfillment, response, or rejection of the request.

We require sufficient authorization before releasing, deleting, or changing, our processing of Personal Data. This is a part of our data security measures that require only appropriate and authorized access to Personal Data. If the requested specific information needed to confirm your identity and authorization to access Personal Data and exercise individual rights over that Personal Data is not provided, then we will not make any disclosures or fulfill any rights in regards to that data.

PRIVACY AFFIRMATION

IT Eagle Eye complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. IT Eagle Eye has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. IT Eagle Eye has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

With respect to personal data received or transferred pursuant to the Data Privacy Frameworks, IT Eagle Eye is subject tot he investigatory and enforcement powers of the U.S. Federal Trade Commission.

INDEPENDENT RESOURCE MECHANISM

In compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), IT Eagle Eye commits to resolve complaints about our collection or use of your personal information transferred to the U.S. pursuant to the EU-U.S. DPF, the UK extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. EU, UK, and Swiss individuals with inquiries or complaints should first contact compliance@iteagleeye.com.

IT Eagle Eye has further committed to refer unresolved DPF Principles-related complaints to a U.S.-based independent dispute resolution mechanism, BBB NATIONAL PROGRAMS. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://www.bbbprograms.org/dpf-complaints for more information and to file a complaint. This service is provided free of charge to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. Please refer to https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf for more information.