RiskIQ Global Privacy Statement

Effective: June 15, 2019

INTRODUCTION

Our Mission

RiskIQ, Inc., including our affiliates ("we", "us" "our" or "RiskIQ") seeks to redefine the global standard for digital cybersecurity risk management beyond the traditional perimeter of a firewall. We provide attack surface-based digital risk protection by illuminating risk associated with an organization's digital presence in open, deep and dark web, mobile, and social digital channels to proactively protect the organization, its brands, people, and data.

Our Sites and Services

We fulfill our mission by providing cloud computing featuring software through a browser interface (primarily SaaS) made extensible by way of APIs, which together with our managed security or professional services whether paid, unpaid, or offered on a trial basis, we refer to individually, or collectively as our 'services' throughout this statement. Through our sites, we also provide information related to our services.

RiskIQ aspires to play an essential role in safeguarding the privacy and personal information of individuals through our sites and services as we seek to fulfill our mission. 'Personal information' for purpose of this statement means any information relating to an individual from which that person is or can be directly or indirectly identified.

When this Statement Applies

This RiskIQ Global Privacy Statement (this "statement") applies to our services and sites that we operate that display this statement. In the event of a conflict between this statement and the terms of any agreement(s) between RiskIQ and our customers, the terms of those agreement(s) shall control. This statement neither applies to the personal information of our business partners, suppliers or other organizations with which we

have or contemplate a business relationship, nor to the personal information of our employees.

PERSONAL INFORMATION WE COLLECT

To fulfill our mission, we collect a wide variety of data that may contain personal information through our sites and services. We collect RiskIQ data from publicly accessible information, either directly, or through others, which may contain personal information. We also collect information from customers (the companies, organizations, or other legal entities that subscribe to, or register to access, any of our services), their respective authorized users of our services, and from visitors to our sites, which may contain personal information, which we individually and collectively refer to as 'your personal information' throughout this statement.

Types of Information We Collect

We collect different types of information that may contain your personal information, such as (i) *Identity and* Contact Info (first and last name, job title or position, physical mailing or delivery address, business email address, phone and fax, area of responsibility, and other similar data that is provided to us when you express interest in, or subscribe to our services, or register to attend one of our events); (ii) Transaction Data (details about orders placed with us, which may include payment information or other information necessary to process your order or verify your payment, as well as account information provided to us when you register through our sites to access our services); (iii) Credentials (usernames and passwords, and any security information used to authenticate access to our sites or services); note that "single sign-on" or "SSO" makes it possible for users to log in without the need to disclose passwords to us, and those credentials are supplied by to the SSO provider, a third party engaged by us, such as Ping Identity Corp., that authenticates the SSO data for authorized users of our services; (iv) Communication Preferences (your preferences related to receiving updates or communications from us, including your individual marketing preferences); (v) Usage Info (current and historical information about how you use our sites or services, which may include technical information about your devices used to access our sites or services, such as operating system or IP address, as well as other information collected by us automatically, such as individual usage details and clickstream data, and other browsing actions and patterns – learn more); (vi) *Service Data* (any data you submit to us for the performance or delivery of the services on your behalf, or that you transmit through the services, or store in the services. This category includes your personal information that a customer (as determined by its authorized users) shares with a restricted set of individuals through its private "project" or "workspace"; (vii) *Other Correspondence* – any other correspondence you submit to us

through our sites that contain your personal information; and (viii) Publicly Shared Data (any of your personal information that you, as an authorized user or visitor, deliberately make publicly available online through our sites or offerings, testimonials, recorded content from training sessions, and other similar contributions that you as an individual choose to make public online (e.g., your contributions to the broader security community through a publicly shared project in PassiveTotal). We recommend that you exercise caution when deciding what to share publicly over the Internet, which is generally an open, global system, where anyone can make copies of a public data item and store it in an arbitrary location; and the public portion of the web does not account for the number, owner or location of such copies.

How We Collect Information

We use different methods to collect information that may contain your personal information, including through:

- *Direct interactions.* You may share your personal information through direct interactions, such as by corresponding with us by post, phone, electronically or otherwise. Examples of how we may receive your personal information through your direct interactions include when you (i) subscribe to one of our services or create an account on one of our sites; (ii) request support or information; (iii) subscribe to our newsletters, or download one of our white papers; (iv) attend one of our trainings or events, or sign up to watch one of our webinars; (v) request a demo or quote in relation to our services; (vi) request marketing materials or sales communications; (vii) complete a voluntary survey to fulfill order expectations, or to improve, enhance, promote or market our services or sites; and when you (viii) give us feedback or contact us.
- *Indirect interactions***.** One of our customer's authorized users may share your personal information with us through various interactions, such as by corresponding with us by post, phone, electronically, or otherwise.
- *Technologies***.** We use various technologies, some of which are automated, to collect and store data, which may have your personal information, including cookies, pixel tags, browser web storage, and server logs. *Learn more*.
- *Third parties or publicly available sources.* We combine different types of your personal information to create customized profiles about you and your organization to form a view on what we think you may want or need, or which of our services are relevant to your organization, some of which we may receive from third parties, such as other users or visitors from your organization, business partners, publicly available sources, or confidential brokers to whom you have recently provided express consent to be contacted by us on behalf of your organization to market our services. Subject to any additional restrictions that also may be imposed by our data suppliers, we seek to only use third-party data in accordance with the practices as described in this statement.

WHY AND HOW WE USE YOUR PERSONAL INFORMATION

Why We Use Your Personal Information

We strive to use personal information that we collect proportionately and responsibly to fulfill our mission through our sites and services. Other than by obtaining your valid consent, we otherwise use your personal information that we collect because we have a contractual necessity to do so, or in furtherance of our legitimate interest not overridden by your individual interests, fundamental rights or freedoms that legally require protection, or because we need to use your personal information to satisfy a legal obligation to which we are subject.

How We Use Your Personal Information

When you request specific information from us, or that we contact you for a specific purpose, we use your personal information that we collect from you to fulfill your request, as well as to assess whether there are new potential customer opportunities, and to market our services to you with your valid consent, whether through our sites by sending you newsletters, or through direct marketing, which may include service recommendations (*learn* how to control our use of your personal information for marketing, and your individual rights).

We use your personal information that we collect to perform our contract with you for the use of our sites and services. When you visit our sites, we also use your personal information that we collect as necessary to operate, administer, develop and improve our sites and services and provide you with the information you access and request, as well as to analyze trends and track your usage of and interactions with our sites to develop and improve our sites and services, and provide more relevant information.

To sustain and grow our business, when you use any of our services, we use your personal information that we collect for (i) account-based marketing to keep you (and any customer for whom you are an authorized user, including its contacts) engaged with us, and to deliver the outcomes reasonably expected, including by enhancing and improving our sites and services; and for (ii) general corporate operations and due diligence in the day-to-day running of our business and planning for our strategic growth.

We use your personal information that we collect to prevent fraud, claims, and other liabilities and to comply with or enforce our legal obligations, and our policies and terms. We also use your personal information that we collect to protect our information, system, network and cyber security, such as preventing unauthorized access, intrusion, misuse or abuse of our systems, networks, computers and information, protecting our intellectual property, and securing our supply chain; for example, if you visit our offices,

we may use camera supervision in accordance with applicable law. We use your personal information that we collect for these purposes where we have a good faith belief that doing so is necessary to protect, exercise or defend our legal rights, or required to comply with a legal obligation to which we are subject.

We reserve the right to use your personal information in furtherance of a merger, reorganization, dissolution or other fundamental corporate change, or in furtherance of a sale of one of our sites or business units, or of a portion of our business assets.

HOW WE SHARE YOUR PERSONAL INFORMATION

We only share your personal information either within the RiskIQ group or with a third-party outside of RiskIQ, as described below.

- within our group, such as with our wholly-owned subsidiary RiskIQ UK Limited (09135597) based in the United Kingdom with offices at 33 Cannon Street, Fourth Floor, City of London EC4M 5SB, England as a co-controller to fulfill your request, or for administrative purposes, such as support, marketing technical operations or account management purposes;
- with our Channel Partners, where you or a person delegated by your organization has subscribed to one or more of our services through a third party, we may need to exchange information with them as part of managing that relationship and your account, including to fulfill your order;
- with our contracted service providers in accordance with our instructions, who are only authorized to use your personal information as strictly necessary to provide services to us;
- with a delegate from your organization that manages your organization's subscription to one of our services and provides you with access as part of the subscription package, or one of its other authorized users;
- with any third-party to comply with a legal obligation to which we are subject, or where doing so is necessary to protect, exercise, or defend our legal rights or to enforce our terms;
- for any stated purpose, when in aggregated form that cannot reasonably be used to identify you;
- to any third party with your prior valid consent;
- to any third party that agrees to use or disclose such personal information consistent with this statement (unless said person obtains your valid consent for other use or

disclosure), where the sharing of such information is in furtherance of a merger, reorganization, dissolution or other fundamental corporate change, or in furtherance of a sale of one of our sites or business units, or of a portion of our business assets; in accordance with applicable laws, we will use reasonable efforts to notify you of any transfer of your personal information to an unaffiliated third party.

OTHER IMPORTANT PRIVACY INFORMATION

Personal Data Security and Retention

As many other institutions have demonstrated, information security can never be assured. We strive to maintain a reasonable, continuous process for implementing, reviewing, improving, and documenting personal information protection. We intend to protect your personal information and to maintain its accuracy by putting in place reasonable physical, administrative, and technical safeguards to help us prevent unauthorized access, use and disclosure. We expect the same from our suppliers, and we are committed to having our security professionals work closely with our privacy team to document that our security systems are appropriate to the risk associated with the loss of confidentiality, integrity and availability of information.

As part of this process, we retain your personal information only as necessary to fulfill the purpose for which we collected it as described in this statement, or possibly longer to the extent doing so is necessary either to protect, exercise, or defend our legal rights, or to comply with our legal obligations.

International Transfers of Your Personal Information

We may transfer your personal information outside of your country of residence within the RiskIQ group as well as to third parties as described in this statement.

We transfer personal information from the European Economic Area and Switzerland to other countries, some of which have not yet been determined by the European Commission to have an adequate level of data protection. For example, their laws may not guarantee you the same rights, or there may not be a privacy supervisory authority capable of addressing your complaints. When we engage in such transfers, we rely on either the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework (including the onward transfer liability provisions), or other lawful measures, such as certain service providers with binding corporate rules that have been approved by the European Commission, or contracts that include the EU *standard contractual clauses*.

EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework

RiskIQ participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework. We are committed to subjecting all personal data received from the European Union (EU) member countries and Switzerland, respectively, in reliance upon each Privacy Shield Framework, to the Frameworks' applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce's Privacy Shield List at *https://www.privacyshield.gov/*.

RiskIQ is responsible for the processing of personal data it receives, under each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. RiskIQ complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data transferred or received pursuant to the Privacy Shield Frameworks, RiskIQ is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If there is any conflict between the terms in this statement and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, visit the *Privacy Shield website*.

If you have a question or complaint related to participation by RiskIQ in the EU-U.S. or Swiss-U.S. Privacy Shield, we encourage you to *contact us*. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at *https://feedback-form.truste.com/watchdog/request*. Under certain conditions more fully described on the Privacy Shield website [https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint] you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Children

We do not knowingly solicit or receive information from children under the age of 16. Please contact us promptly if you believe we might have collected any information from a child under the applicable age of consent in your country, so that we may appropriately investigate and address the issue.

Updates to this Statement

We may update this statement when we believe it is necessary. Please refer to the "Effective Date" at the top of this statement. You can access prior versions to track the changes we have made. If we make any material changes, we will notify you by prominently posting a notice before the changes will take effect, or by directly sending you a notification. We encourage you to periodically review this statement to keep track of any changes to this statement.

Websites Linked to from our Sites and other Third-Party Services

We may provide hyperlinks to other sites for your convenience that are not covered by this statement. If you click on any such hyperlink, we recommend that you read the relevant privacy notice to make sure you are comfortable with the applicable privacy and data security practices that govern, which may be different than as described in this statement.

Similarly, when you connect or enable a third-party application, database, software or service together with our services (including one that is integrated by you or at your direction), we recommend you review the applicable privacy notice.

More about cookies and tracking technologies

Like most websites, we record page requests made from our visitors in "server logs" that may include your personal information. We typically keep server logs for up to 90 days.

We also use "local storage" to store data in your browser across sessions—even after your browser has been closed and reopened. We deliver files from our sites and services through your browser that contain site data ('cookies' or 'trackers'), which are stored on your computer, either as set by us directly, or by one of our suppliers we have entrusted. We recommend managing these cookies using the browser functions in your browser (typically, under "options" or "settings") if this is important to you, but you may not have the visibility to do so from your mobile device.

You can selectively use browser plug-ins or add-ons to add privacy-enhancing capabilities to your browser, such as *Cookie Auto-Delete* and *uBlock Origin*. You should make sure you are comfortable with the privacy practices of any such third-party browser add-ons. All popular browsers have help documentation available on how to adjust your cookie settings. We also recommend choosing your browser selectively if greater flexibility for privacy customizations is important to you.

Some of the files we deliver through your browser are required information. Therefore, while you may have the technical option of disabling all files from being stored on your computer through your browser settings, you should be aware that if you disable all cookies or other site data, which includes those that are **required**, you will no longer be able to use some functions or features on our sites or services. For example, we use cookies for session management, which is required for our services to be redundant to the failure of any one server. Without this, users would also have to provide a username and password on every screen, and we would not be able to track the completion of downloads from our services, so that our subscribers can export data from our services as intended.

If you use our services or visit our sites, some of the **analytical cookies** we use are required for error and connectivity monitoring, logging and analytics, event tracking for service improvement, and support. We also use cookies to interact with you while you are using our services or visiting our sites. If you choose to disable any of these cookies, we will no longer be able deliver our services as intended. We recommend that you address any concerns you may have as an authorized user directly with our customer. For example, without *Google Tag Manager*, other scripts that are loaded into the page may no longer function. If you disable *Google Analytics*, you may impair our ability to monitor our performance when you visit our sites.

We also use some cookies that may contain some of your personal information on our sites and in some of our services in furtherance of our legitimate interests in customer analytics and/or account-based marketing, such as through *Woopra* and/or *Marketo*.

In furtherance of our legitimate marketing-related interests, we also partner with third parties to deliver **advertising cookies** to those visiting our sites in order to display advertising on our sites and to manage advertising on other sites. Examples include cookies we deliver through DoubleClick and Twitter. If you wish to opt out of interest-based advertising, click *here* [or if located in the European Union, click *here*].

Apart from following the instructions on how to manage cookies in your browser, we also provide a way you may be able to adjust some of your preferences through a third-party cookie consent manager here. This is made available to you at your own risk. A downside of this may be that you must allow third-party cookies in your browser settings to use it, and some of the opt-outs may fail, including due to your cookie settings in your browser. It also may not necessarily be up to date, depending on when we last reviewed the scans, and how often those scans occur.

Your Rights as an Individual

We respect your rights and control over your personal data. You may exercise any of the following rights as the law allows (which means under some circumstances, there

may be legal or official reasons that we may not be able to fully address the specific request you make) by *contacting us*. Please note that for security purposes, we may ask you to verify your identity before taking further action on your request. We aim to respond to your request within 30 days, or otherwise within a reasonable timeframe under the circumstances subject to applicable law.

Right of Access – the right to verify the accuracy of your personal information that we hold about you upon your request, including to the right to be informed of and request access to personal information we process about you;

Right to Rectification – the right to amend or update your personal information upon your request where it is inaccurate or incomplete;

Right to Erasure – the right to have your personal information deleted upon your request without undue delay under any of the following circumstances with respect to your personal information: (i) it is inaccurate, (ii) it is no longer necessary in relation to the purpose for which it was collected or otherwise used, (iii) there are no overriding valid legitimate grounds that we rely on for using your personal information and you have objected, (iv) it has been unlawfully used; or (v) it is required to be erased to comply with a valid legal obligation.

Right to Restrict – the right that we temporarily or permanently stop processing all or some of your personal information in certain situations upon your request, such as to verify its accuracy or where the processing is unlawful and you object to erasing it, or where we no longer need your personal information but you need it for certain valid legitimate interests or to comply with a legal obligation, or pending verification whether there is a valid legitimate grounds for processing your personal information over your objection.

Right to Object – the right at any time (1) on grounds relating to your particular situation to object that our processing of your personal information for our valid legitimate interests is not compelling, in which case we will no longer process your personal information unless (i) we demonstrate our interests are still valid because they outweigh your rights and freedoms taking your particular situation into account, or (ii) continuing to process your personal information is necessary to protect, exercise or defend our legal rights; you also have the right (2) to stop your personal information from being processed by us for direct marketing purposes upon your request.

Direct Marketing – Exercising Your Right to Object

You may choose to exercise your right to object to direct marketing by *contacting us*. You can also opt-out of any direct marketing electronic newsletters by using the 'unsubscribe' functionality at the bottom of our emails. You can also opt-out of

marketing phone calls (we do not use automated means) by telling our representative to add you to our “Do Not Call” list. You may *contact us* to opt out of receiving any postal mail.

Right to Data Portability – the right to receive upon your request, a copy of your personal information that we are processing by automated means or based on your valid consent, and to transmit it to a different controller without hindrance from us, in a structured, commonly used and machine-readable format, or directly from us to a different controller, where technically feasible.

Right not to be subject to Automated Decision-making – We do not subject you to any decision based solely on automated processing of your personal information,

In addition to the rights you may have subject to and in accordance with applicable law, as set forth above in this statement with respect to access, updating or correcting your personal information, as well as objecting to direct marketing, you may have other rights pursuant to your local law applicable to the processing.

Furthermore, in the event you consider our processing of your personal information to infringe on your rights pursuant to applicable data protection laws, please lodge a complaint with us by contacting us below. Without prejudice to any other rights you may have, you may also lodge a complaint with your local or other competent data protection authority. Contact details for data protection authorities in the European Economic Area (EEA) are available *here*, including for the Information Commissioner’s Office, which is where we have our main establishment within the EEA.

If you wish to exercise any of your individual rights as an authorized user with respect to your personal information that we process on behalf of our customer, we request that you first contact our customer as the data controller. We cannot assume responsibility for the privacy or security practices of our customer, which may be different than as described in this statement.

Contact Us

If you have support-related questions, comments or concerns with our services or to close your account, please contact us via *support@riskiq.com*.

If you have any questions, comments or concerns with this statement, or our privacy or data protection practices, please email *privacy@riskiq.com*.

You can also contact us at +1.888.415.4447 to leave a message for our Personal Data Protection Team. If you are still unsatisfied, you may contact our legal department via *legal@riskiq.com*. We will respond to questions or concerns within 30 days, or otherwise within a reasonable timeframe under the circumstances subject to applicable law.

For the purposes of the EU General Data Protection Regulation (GDPR), the controller of your personal information is RiskIQ, Inc., 11 Battery Street – 10th floor, San Francisco, California, United States 94111, unless indicated otherwise. RiskIQ UK Limited in the United Kingdom is a co-controller of personal data when it transfers personal data that is processed in connection with certain legitimate interests we have in marketing and sales, and day-to-day business operations, including information collected from its offices in London.