LAST MODIFIED: MAY 11 2018

Data Privacy & Governance Policy

FLEXIBLE NETWORKS NORDC, Mäster Samuelsgatan 60, SE-111 21 Stockholm, Sweden +46 8 546 584 30 info@flexinets.se

iPASS , 3800 Bridge Parkway, Suite 200, Redwood Shores CA 94065 United States +1 650 232 4100 privacy@ipass.com

Effective Date: May 11, 2018

This Privacy Policy provides information about data we collect, use, and share, and our commitment to using the personal data we collect in a respectful fashion.

We at iPass, Inc. (“iPass”, “we”, “us”) care deeply about privacy, security, and online safety, all of which are a significant part of our essential mission: to provide users of our products and services (“you”, “your”) with global mobile connectivity technology that keeps people and things securely connected to the best network available. At iPass, we design our mobile application products and services according to the principle of privacy by default and collect only the minimum amount of data necessary to provide our users with a product or service. This Privacy Policy (“Policy”) is designed to inform you about how we collect, use, and share your personal information.

This Privacy Policy applies to personal information we obtain from our customers (“Business Clients”) and individuals through our websites, products, mobile applications (“Apps”) and services (collectively, the “Services”).

When you access or use our Services, you acknowledge that you have read this Policy and understand its contents. Your use of our Services and any dispute over privacy is subject to this Policy and our Terms of Service (including any applicable limitations on damages and the resolution of disputes).

As iPass evolves, our business may change, and we may update this Policy at any time as we deem appropriate to reflect those changes. Where the changes are material, we will post them here in advance and, if the changes are likely to affect you personally, we will also attempt to contact you directly (such as via email if we have your email address). It is important that you check back from time to time and make sure that you have reviewed the most current version of this Policy.

Why Do We Collect Information and Data?

We rely on certain information to run our business. In some instances, this information may include data that could be used to identify a particular individual, otherwise referred to as Personal Information. In this Policy, we will provide multiple examples of how Personal Information we collect may be used and why it is important. For example, Business Clients of iPass may provide iPass with Personal Information to help iPass provide its Services to customers or employees of the Business Clients. Some of the reasons that we collect Personal Information include to:

- Provide our products and services, including our Apps and our website (“Site”), and improve them over time;
- Personalize and manage our relationship with you, including providing customer support;
- Investigate, respond to, and manage inquiries or events; and
- Work with and respond to law enforcement and regulators.

What Kinds of Personal Information Do We Collect?

The following are examples of the type of Personal Information that may be collected. The specific kind of information collected will depend on the Services used:

- Authentication information (including email address and password);
- Device information (including unique identifiers for computers, tablets or phones to confirm their eligibility for use of the Service);
- Session data (including access point information and location information for the purpose of enabling the Service to connect users to the best available connection).
- Optional data (at the direction of iPass Business Clients, iPass may collect user names for billing and eligibility purposes and Ad-ID)

Session Data, including aggregate usage statistics, is generally not personally identifying. On the other hand, some of this Session Data either alone or when combined or linked with your Personal Information, may allow your identity to be discovered. In such cases, we treat the combined data as Personal Information. In many cases, Session Data is gathered automatically by systems or technology such as cookies (see the section on Information Collected Automatically below).

How Do We Collect Information?

We collect information from our Business Clients in order to provide the Services to you on their behalf, automatically through your use of our Services and, in some cases, directly from you.

For personal data subject to the European Union’s General Data Protection Regulation (“GDPR”), we rely on several legal bases to process the data. These include when the processing is necessary to perform a contract, for compliance with a legal obligation to which iPass is subject, and for our legitimate business interests, such as in improving, personalizing, and developing the Services, and promoting safety and security as described above.

Our Site may contain publicly accessible blogs or community forums. You should be aware that any information provided in these areas may be read, collected and used by others who

access them. To request removal of any Personal Information for our blog or community forum, contact us at privacy@ipass.com.

Site Information Collected Automatically: When you use or interact with our Site we receive and store information generated by your activity, like Session Data, and other information automatically collected from your browser or mobile device. This information may include your IP address; browser type and version; preferred language; geographic location using IP address, the location of an access point you access while using the Service, or the GPS or wireless technology on your device; operating system and computer platform; purchase history; the full Uniform Resource Locator (URL) clickstream to, through, and from our Site, including date and time; any searches you conducted; and areas of our Site that you visited. We also may log the length of time of your visit and the number of times you visit and purchase or use the Services. We may assign you one or more unique identifiers to help keep track of your future visits.

In most cases, this information is generated by various tracking technologies. Tracking technologies may include “cookies,” “flash LSOs,” “web beacons” or “web bugs,” and “clear GIFs”. You can read about how we use cookies and other tracking technologies in our Cookie Notice and also learn about the choices you can make to limit their use.

How Do We Use Personal Information?

Provision of the Service.
iPass will use Personal Information only for purposes related to providing you with the Service on behalf of iPass Business Clients or otherwise to improve the Service. iPass will use and process your Personal Information: (a) in connection with provisioning of the Service; (b) to incorporate your data into databases controlled by iPass for administration, provisioning, billing and reconciliation, verification of your identity, maintenance, support and product development, fraud detection and prevention, customer and customer use analysis and reporting and customer-directed application of policies as part of our service delivery. iPass may also use Session Data to contact third parties in connection with inappropriate use of the Service or violation of iPass policy.

Business Uses.
We may use Personal Information for business purposes, including to:

- Analyze users’ behavior when using iPass products and services to customize preferences;
- Establish and manage iPass accounts;
- Provide customer support, manage subscriptions, and respond to requests, questions, and comments;
- Customize, measure, and improve our websites, products, services, and advertising;

- Prevent, detect, identify, investigate, respond, and protect against potential or actual claims, liabilities, prohibited behavior, and criminal activity;
- Comply with and enforce applicable legal requirements, agreements, and policies; and
- Perform other activities consistent with this Policy.

Processing as Part of the Services.
We also process certain information as an integral part of our Services. If you install one of our Apps or use one of our services, software will operate in the background of your computer system or device environment to perform specific tasks including:

- Determining the quality of available network access points;
- Intrusion detection, prevention, and protection;
- Network defense; and
- Data encryption.

When Do We Share Personal Information?

We respect the importance of privacy. Other than as provided in this Policy, we do not sell your Personal Information, nor do we share it with unaffiliated third parties for their own marketing use, unless we have your consent or we are required by law to do so. Generally, we may disclose the information we collect, including Personal Information, in order to facilitate our provision of the Services or communications with customers (e.g., to service providers who perform functions on our behalf), to operate our business, to advertise or promote our Services, to facilitate changes to or transfers of our business, as required by law, or with your consent.

We may share Personal Information in the following ways:

- Current and future members of the iPass family of companies for the purposes described in this Policy, such as to: (i) provide services (e.g., registration, and customer support); (ii) help detect and prevent illegal acts and violations of our policies; and (iii) guide our decisions about our products, services, and communications;
- Authorized service providers who perform services for us (including cloud services, data storage, customer support, and bill collection). Our contracts with our service providers include commitments that they agree to limit their use of Personal Information and to comply with privacy and security standards at least as stringent as the terms of this Privacy Policy. Remember that if you provide Personal Information directly to a third party, such as through a link on from the Service, the processing is typically based on their standards (which may not be the same as iPass');
- If we believe disclosure is necessary and appropriate to prevent physical, financial, or other harm, injury, or loss, including to protect against fraud.

- To legal, governmental, or judicial authorities, as instructed or required by those authorities or applicable laws, or in relation to a legal activity, such as in response to a subpoena or investigating suspected illicit activity (including identifying those who use our services for illegal activities). We reserve the right to report to law enforcement agencies activities that we in good faith believe to be illegal.
- In connection with, or during negotiations of, an acquisition, merger, asset sale, or other similar business transfer that involves substantially all of our assets or functions where Personal Information is transferred or shared as part of the business assets (provided that iPass will continue to take measures to protect the confidentiality of Personal Information and give affected users notice before transferring any personal information to a new entity).
- With others after obtaining your consent. If we want to share Personal Information other than as permitted or described in this Policy, we will provide you with a choice to opt in to such sharing and you may choose to instruct us not to share the information.

  iPass does not share your Personal Information with non-affiliated third parties for their own marketing use without your permission.

  We may disclose to third parties Session Data or non-Personal Information that is aggregated or de-identified so that it cannot reasonably be used to identify an individual.

What Security Measures Do We Have?

We use administrative, organizational, technical, and physical safeguards to protect the Personal Information we collect and process. Our security controls are designed to maintain an appropriate level of data confidentiality, integrity, and availability. We regularly test our website, data centers, systems, and other assets for security vulnerabilities.

iPass uses commercially reasonable protection technology such as encryption (when you provide us with information such as login credentials), firewalls and other security procedures to help protect the accuracy and security of your Personal Information and Session Data and to help prevent unauthorized access or improper use.

What Control do I have over my Personal Information?

Because iPass provides the Service to you on behalf of its Business Clients pursuant to contract, users should contact the Business Client directly to request correction, access, or deletion of Personal Information associated with your account. If the Business Client then requests iPass comply with your request, iPass will respond to the request within 30 business days.

Data Retention
We retain your Personal Information while your account is in existence or as needed to provide you the Service. This includes data you or others provided to us and data generated from your

use of the Service. In some cases we choose to retain certain information in a de-identified or aggregated form.

Our International Operations and Data Transfers
We operate internationally and may transfer information collected within the European Economic Area and Switzerland to the United States for the purposes described in this policy.

We are subject to the oversight of the US Federal Trade Commission and remain responsible for personal information that we transfer to others who process it on our behalf.

Links to Other Websites and Services
Our Site or Services may contain links to other websites or services for your convenience and information. These websites or services may be operated by companies not affiliated with iPass. Linked websites or services may have their own privacy policies or notices, which we strongly suggest you review if you visit those websites. We are not responsible for the content, privacy practices, or use of any websites that are not affiliated with iPass.

iPass does not control the third-party sites that may be accessible through the Site or through the use of the Services. Thus, this Privacy Policy does not apply to information provided to third-party sites or gathered by the third parties that operate them. Before visiting a third-party site and before providing any information to any third party, you should inform yourself of the privacy policies and practices of the third party, and should take those steps necessary, in your discretion, to protect your privacy.

Other Languages
This document has been translated into the local language for informational purposes only. In the event of any discrepancy between the translated version and the English version, the English version shall be controlling.

Contact Us
With regards to any handling of your Personal Information, iPass acts primarily as a processor on behalf of its Business Clients, who act as the controller. Please direct any inquiries to the Business Client that engaged iPass to provide you with the Service.

For instances in which iPass acts as a controller of your Personal Information, or if you have questions or concerns regarding this Privacy Policy, please contact us by email at privacy@ipass.com or by writing to us at:

Attn: Legal Department
3800 Bridge Parkway, Suite 200
Redwood Shores, CA 94065

Privacy Governance Policy Statement

At iPass we design our mobile application products and services according to the principle of privacy by default and collect only the minimum amount of data necessary to provide our users with a product or service. This data is also necessary to bill our services accurately and completely to the contracting commercial entity, be that enterprises or channel resellers. iPass rarely contracts directly with end-consumers for our products or services, but we do publish a "terms of use" and "privacy policy" inside every iPass SmartConnect™ app that is downloaded under a commercial agreement with an enterprise or channel reseller. For the limited number of end-user renewals that we take direct from consumers, we outsource all payment processing to a third party application and maintain only limited, non-sensitive personal data. We take personal rights seriously and strive to be thoughtful and transparent in how we use and protect our users' personal data.

iPass collects information from users under three primary lawful bases:

- Processing is necessary for the performance of a contract, or
- Processing is necessary for compliance with a legal obligation to which iPass is subject, or
- Processing is necessary for the purposes of the legitimate interests pursued by iPass or a third party in providing our services.

Personal data is any information relating to an identified or identifiable person ("data subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity. As a data processor, iPass has several attributes of personal data that are integral to the operation of the iPass SmartConnect™ technology:

Personal Data – data that can be identified or identifiable with a person; this information is required in order to authenticate and access the service.

- **Email addresses** – used to provision and authenticate end-users; can be associated with a customer name via domain.
- **Passwords** – used to provision and authenticate end-users. Passwords are encrypted, one-way hashed, and stored in lightweight directory access protocol (LDAP) format. Our preference is to use one-time passwords that have no linkage to any other user security passwords, but we can provision authentication based on customer required standards.
- **Device ID** – unique identifier of a laptop, tablet, or phone that by reference to other personal data could be mapped to an identifiable person.

Session Data – data that is required for the service to function as designed and intended. Note, on its own, most of this data is likely not personal data, but once cross-referenced to email addresses or device IDs, it is possible this data could be indirectly attributed to an identifiable person.

- **Location Services** – latitude and longitude readings of iPass SmartConnect enabled devices that are connecting or attempting to connect to a Wi-Fi or other access point. This data is critical to identifying, authenticating, and connecting to a valid access point in the iPass global network.
- **Access Point IP Address** – our service connects users to Wi-Fi access points, and IP addresses are necessary to identify and authenticate a user against an access point.
- **Service Set Identifier (SSID)** – unique name of a wireless local area network (WLAN).
- **Basic Service Set Identifier (BSSID)** – media access control (MAC) address of the WLAN access point or network interface controller (NIC).

Optional Data – this data is not required to access the service or for the service to function as designed and intended.

- **End-user Names** – not necessary for operability of the iPass service but is often provisioned by the enterprise customers in order to simplify the billing and reporting process.
- **Ad-ID** – the advertising industry standard unique identifier for all commercial assets; currently iPass does not gather this data unless requested under a specific commercial arrangement with a customer.

The non-optional attributes are critical to the operation of our services, and without any of this data, the end-user could not use the iPass service for its intended and contracted purpose, to connect a mobile device to the best available internet connection. Without this data, or if the data subject opts to object to the processing of this data, the service will no longer work for that user. Any objection by a data subject should be directed to the enterprise that contracted for the iPass service. If a user objects to iPass directly, we will ensure your objection is forwarded timely to the appropriate controlling party for resolution.

The optional attributes address specific use cases. In our product, we do not collect any directly identifiable sensitive personal data and have never been subject to any Personal Identifiable Information (“PII”) or Sensitive Personal Information (“SPI”) regulations. To the extent these use cases were to be developed in later iPass products, we would likely implement an opt-in consent mechanism to support any direct marketing of personal data.

iPass may package and provide a business customers service data, including personal information pertaining to its end users, as part of the customer’s Veri-Fi service. In this case, iPass functions as a data processor to its controller business customers. Additionally, iPass may anonymize service data and share non-identifiable data to other customers. As these data

do not fall under the definition of personal information under the GDPR, iPass is neither a processor nor a controller of personal information.

To make sure personal data is secure, we strictly enforce privacy safeguards within the company. This means we use access management and access controls commensurate with the risk to data to ensure access to data is associated with a business need, such as providing customer support. Data sold under Veri-Fi is delivered anonymized to the customer or pseudonymized to the customer if the personal data is related to its own employees or end-users. In the latter case, we are operating purely as a data processor on behalf of the data controller (the customer).

If iPass becomes aware that it may have experienced a reportable data security breach that might impact our users' personal data, we investigate to learn what happened and determine what steps to take in response. We analyze these facts — in the context of applicable laws, regulations, industry norms, and most of all iPass' established commitment to privacy — to determine whether we should notify affected customers, or other relevant parties like regulators. iPass complies with all applicable laws that require notification about data security incidents.

###

Frequently Asked Questions (iPass and EU General Data Protection Regulation or "GDPR")

1. **Will iPass need to obtain consent from end-users to provision new users or continue to offer its core intelligent connection management services to existing users?**
   The personal data gathered to provision and deliver the iPass service to B2B and B2B2C end-users (identified or identifiable persons) is covered under Article 6 of GDPR "Lawfulness of Processing." Under this provision, processing of personal data attributes (email addresses, passwords, device ID, location services, IP address, SSID, and BSSID) is necessary for the performance of a contract, with either an enterprise or a channel reseller, to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
2. **Will any new products offered by iPass require affirmative consent from end-users?**
   Currently NO. Our Veri-Fi™ big data products include selling anonymized network quality of service data metrics to various mobile carriers and mobile virtual network operators. The raw data is scrubbed of all personal data and is intended to provide aggregating statistics on network availability, capacity

planning, investment decision making, and other big picture connectivity related topics. This data will not require user consent.

Future products MAYBE. We will not share, sell, license, rent, or otherwise permit access to personal data that individually and personally identifies a person to an unaffiliated third party for that third party to market its products or services to you unless we have the required consent to do so.

3. **What are the key access controls that iPass has in place to ensure personal data is secured?**
    - Role-based access to systems and databases approved via internal workflow.
    - Multi-Factor Authentication to get access to production servers.
    - Data encrypted when at rest at the hardware level.
    - Entry controls to restrict access to premises and equipment in order to prevent unauthorized physical access, damage, and interference of personal data at our SOC 2.0 certified data centers and corporate headquarters.
    - Written policy to securely dispose or destroy data and equipment when no longer required.
    - Clear defined and documented internal ownership of software and hardware assets.
    - Secured mobile devices like laptops with disk level encryption to protect from theft or loss.
    - Continues scanning of hardware and software to reduce vulnerabilities and process only required functional service.
    - Fully defined and documented password security procedures and rules for information systems, including monitoring attempted unauthorized access or anomalous use.
    - IDS (Intrusion Detection Sensors) and IPS (Intrusion Prevention Sensors) in place to detect and prevent harmful security breaches.
    - Monitor user and system activity to identify and help prevent data breaches.
    - Documented and published process to identify, report, manage and resolve any security or data breaches.
4. **Will iPass need to update its end-user and commercial terms and conditions prior to GDPR go-live (May 25, 2018)?**
   YES. While our ***terms of use*** and ***privacy policy*** are well documented and included in our commercial terms and conditions, we will update the policy to ensure all relevant GDPR requirements are included. For example, our policy will establish, record, and inform subjects about the lawful basis iPass is relying on to process necessary personal data. The policies are available for review on our website (iPass.com), in our mobile applications, and on our customer portal. These policies will be updated regularly for any changes.
5. **How does iPass ensure compliance with the requirements of GDPR?**
   iPass has identified a Data Protection Officer (DPO), who is also the general counsel of the corporation. In addition, iPass has a privacy steering committee made up of key leaders from executive management, engineering, legal, and operations to ensure privacy issues are properly addressed in the design, development, and operation of our products and services. Under the steering committee,

subject matter experts (SMEs) are assigned from each functional area impacted within the organization. Regular meetings are held, training provided, and policies updated to ensure iPass remains current on privacy governance.

In addition, we include privacy requirements in our commercial contracts with customers, partners, and vendors. We clearly identify the responsibilities of data controllers, data processors, and the records of processing activities to ensure both parties are informed and aware of iPass' emphasis on data privacy.

6. **Did iPass assess its compliance with GDPR with the assistance of any professional organizations?**
   YES. We engaged TrustArc to oversee our compliance initiatives. At the direction of TrustArc, we assessed our environment, reviewed our risk areas and gaps, created an internal awareness campaign, designed and implemented new operational controls, and created a maintenance and enhancement program for our key controls. We engaged our customers and vendors in this process to ensure we were meeting the requirements of all our stakeholders.

7. **How will iPass deal with the various rights to object, such as "Right to Access" and "Right to be Forgotten" of data subjects?**
   A user can contact the iPass Data Protection Officer at:

   iPass Inc. (Data Protection Officer – Legal Department)
   3800 Bridge Parkway
   Redwood Shores, CA (USA) 94065

   Objections will be forwarded in a timely manner to the commercial contact at the related contracting customer for resolution.

8. **Beyond the implications of GDPR for iPass products and services, is iPass intending to be GDPR compliant across all corporate functional areas?**
   YES. The cross functional teams (e.g., marketing, sales, legal, engineering, operations, and general & administrative) have each assigned subject matter experts (SME) to the project. Each SME is responsible for understanding the implications of GDPR in their respective functional areas, at the direction of the Project Lead, and training their teams on the appropriate controls, processes, and procedures to ensure adequate protection of all data from privacy breaches.

9. **What is the difference between a "data controller" and a "data processor" and how is iPass impacted?**
   iPass is a data processor when providing the goods and services (e.g., iPass SmartConnect, Veri-Fi) to our contracted enterprise customers. iPass is a data controller when using data to operate the iPass SmartConnect data driven software optimization or resell aggregated and anonymized data to unrelated third parties. Non-anonymized personal data is never resold to unrelated third parties.

10. **How long is personal data kept by iPass?**
    As long as necessary to continue to deliver the service, support billings to customers, and meet financial and related record retention statutes. Once an enterprise customer terminates service with iPass, all personal data is fully anonymized and used only in Quality Assurance (QA) and Development environments to continue to provide data driven insights on the quality of service delivery.

11. **Does iPass transfer data cross-border or out of the EU?**

    YES. All identifiable personal data is resident in the United States but in order to authenticate users and provide the service, device and network specific data must be transferred through transaction servers and the cloud to our colocation facilities in the United States. No sensitive personal data is transmitted across borders, and iPass is compliant with EU-US Privacy Shield, and the predecessor US-EU and US-Swiss Safe Harbor Frameworks. Our iPass SmartConnect software includes Last Mile VPN security to ensure any data transferred between a connecting device and the access point is properly secured.