iPass Inc. Privacy Governance Policy

Privacy 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:

1) Processing is necessary for the performance of a contract, or
2) Processing is necessary for compliance with a legal obligation to which iPass is subject, or
3) 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?**
   NO. 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.