InCountry

FAQ
Security and Compliance

Question	Response
What is InCountry?	InCountry provides data residency-as-a-service in more than 90 countries for sensitive and regulated data, ensuring customers comply with local data protection regulations. InCountry's end-to-end data stack, from infrastructure to data compliance, is for global companies looking to utilize cloud and SaaS solutions while still ensuring data compliance in countries they operate in.
How is InCountry different from hosting?	InCountry's platform allows companies to comply with various data regulations and data residency requirements by enabling sensitive and regulated data to be localized. InCountry's first-of-its-kind data stack starts with providing certified cloud infrastructure, all the way to SaaS and data integration and compliance with local regulations. In this way, InCountry's cloud-agnostic platform ensures only the data that matters is localized, while the rest is still in customers' existing data centers. This model makes data localization an efficient and straightforward process that can be replicated easily to multiple countries.
What SaaS solutions does InCountry support?	InCountry supports Salesforce, ServiceNow, Mambu, Segment, Twilio, and other SaaS solutions. In addition, Contact Sales at sales@incountry.com to investigate the possibility to support your application.
How does InCountry help with a multi-country SaaS implementations?	InCountry's availability in 90+ countries means customers can utilize the same platform to localize different types of data with the same way it takes to localize in one country. This provides customers quick time-to-value through repeatable and fast on-boarding. For more information, please visit https://incountry.com/products/saas/.
Does InCountry support internal applications?	Besides supporting SaaS solutions, InCountry supports internal applications using our SDK toolkit. For more information, please visit https://incountry.com/products/internal-apps/.

InCountry -- FAQ
Security and Compliance

Question	Response
What is InCountry's hosting model?	InCountry is responsible for providing the complete data stack, including infrastructure, application integration and local compliance. InCountry's platform is isolated and secured based on the customer's needs. Our offerings vary from multi-tenant infrastructure to completely isolated single-tenant hosts with a dedicated resource pool within a secure and compliant environment. Depending on the customer's needs and availability, the InCountry platform can run on the cloud provider of choice. Except in the case of InCountry self-hosting offering, Corporate Node On-prem, For more information, please visit https://incountry.com/products/overview/.
What is the role of cloud providers with InCountry's platform?	InCountry utilizes cloud providers, big and small, as part of our data stack. We ensure every cloud provider we use is of high standards, security, and compliance requirements. For more information, check out our compliance and security page. Our solutions include all the infrastructure equipment is provided by InCountry, regardless of the cloud/infrastructure provider. InCountry ensures the provider is compliant with the required certifications and attestations.
How secure is the InCountry platform?	InCountry provides enterprise-grade, industry-standard security. InCountry's facilities offer enterprise-class security, with enterprise-class protection including data encryption, firewalling, network isolation, and intrusion detection. Additionally, high availability and disaster recovery capabilities are included as part of our managed services offering.
Which security standards do InCountry offerings adhere to?	Besides the adherence to multiple security and compliance standards and best practices, like SOC 2, PCI DSS and HIPAA, InCountry adheres to strict and robust security and compliance requirements, both internally and externally. We hold ourselves to a high standard when it comes to securing our data and customer's data. With continuous programs and training, we ensure our employees, regardless of their duties, are up to date with the industry's latest requirements and standards.
What kind of security testing does InCountry perform, and how often?	In compliance with our standards and audit requirements, all equipment within our systems is constantly scanned for vulnerabilities on at least a monthly basis. In addition, 3rd parties assess our systems for compliance with different security and privacy standards annually, which includes vulnerability scans, application penetration testing, and network segmentation testing.

Question	Response
Do InCountry employees working / supporting / developing the solution have background checks?	Minimal and limited personnel have access to support and administer InCountry systems. All InCountry employees successfully pass a background check.
Is InCountry able to access the customer's data?	InCountry focuses on the protection of customer data and intellectual property (IP). Therefore, general security protection mechanisms apply to protect customer's data and IP. Access to strictly confidential information is limited to a small number of precisely specified persons based on the need-to-know principle. In general, user management for InCountry is controlled using well-known and trusted GRC solutions. Furthermore, InCountry administrators have no direct access to customer data.
Which security regulations are applicable for InCountry?	Information Security is not just a buzzword for InCountry – it's our daily work, our passion, and the principle that drives us. InCountry is currently SOC 2 Type II audited and will be certified against internationally-recognized standards such as ISO 27001 for Information Security (Planned for Fall 2020). Globally, InCountry is compliant with local data regulations in operational countries. All these, along with using industry-accepted best practices, ensure that the best possible security and risk management approach is applied. InCountry's security and compliance program is always extending more certifications and attestations, and conducting technical security audits regularly to validate that the defined security concepts have been implemented successfully, and to safeguard the usage of newly-developed tools. The external certifications and attestations are performed by Coalfire and NSF-ISR, two highly recognized audit firms
Where are the data centers located?	InCountry's platform is available in 90+ countries. Please contact sales for more specific information on the data center location.
What is the physical data center security?	We ensure all data center facilities we use are of at least Tier III level and are at the minimum certified with ISO27001 or SOC2. The InCountry platform can be deployed on the data center host provider of choice, if the customer has any.
What type of encryption is used by InCountry?	InCountry uses SHA-256 for hashes and AES-256 for data payloads.
How will the transmission of data from our out of country applications to the "in the country" InCountry platform - be safeguarded?	Data will be encrypted for transmissions between the customer and InCountry nodes both at rest and in transit. The encryption technologies are SHA-256 and AES-256.

Question	Response
Does InCountry work with third party key management system?	Yes, InCountry integrates with third party enterprise key management solutions (KMS) provided by third-party vendors and supports bring-your-own-key(BYOK) scenarios.
Is InCountry able to access the customer's data?	Access to customer data shall not be provided to InCountry employees unless authorized in writing by the customer or provided for in the parties' SOW. InCountry focuses on the protection of customer data and intellectual property (IP). Therefore, general security protection mechanisms apply to protect customer's data and IP. Access to strictly confidential information is limited to a small number of precisely specified persons based on the need-to-know principle. In general, user management for InCountry is controlled using well-known and trusted GRC solutions. Furthermore, InCountry administrators have no direct access to customer data.
Who owns the data? How will the data be handled in case of contract termination?	The customer owns their data. In the case of contract termination, InCountry will retain the customer data as agreed in the contract for data retrieval purposes or migration. Post data retention interval InCountry deletes customer data on the InCountry platform and all relevant storage infrastructure. InCountry deletes the logical volumes, which will cause the storage device to re-use the storage space and overwrite the customer data.
Describe the InCountry backup capabilities and tools.	InCountry has a formal system backup policy and schedule, which includes hardware independent restore and recovery capabilities. Incremental and full backups are performed for all customer data
How does the InCountry platform address disaster recovery (DR) requirements?	InCountry's platform includes disaster recovery and other business continuity capabilities. The plans are periodically tested, reviewed for potential enhancements by InCountry and external auditors, and updated if required.
Can InCountry provide SOC 2 and SOC 3 reports?	Yes. SOC 2 is available for interested prospects and SOC 3 is publically available here https://incountry.com/products/compliance-and-security/.
What is InCountry's stand on GDPR?	InCountry is committed to ensuring its compliance as a company with the requirements of the General Data Protection Regulation (GDPR). InCountry provides services to customers worldwide based on robust security, privacy, data protection, and contractual foundation. To validate InCountry's commitment to the GDPR requirements and overall security, privacy, and data protection InCountry has achieved ISO/IEC 27001:2013 certification and validated conformance with ISO/IEC 27017:2015, 27018:2019 & 27701:2019. The ISO standards are globally recognized, risk-based standards an organization, information security standard providing a set security objectives an organization must achieve as well as the implementation of an overall Information Security Management System (ISMS). This internationally recognized standard is the basis of many other security standards as well as local regulatory requirements.

InCountry -- FAQ

Security and Compliance

Question	Response
What does this mean for InCountry and the InCountry platform?	• Validation by independent 3rd party auditors provides additional validation of InCountry's continued commitment to the principles of security, privacy, and data protection. • With the combination of ISO/IEC 27001:2013, ISO/IEC 27017:2015, 27018:2019 & 27701:2019 InCountry effectively demonstrates to customers and other external parties the level of commitment InCountry has to meet the requirements of the GDPR. • ISO/IEC 27001:2013 is focused on Information Security and helps to ensure InCountry has a formal information security and risk management program which includes an internationally agreed-upon set of objectives and requirements. • ISO/IEC 27701:2019 provides a set of requirements for developing a PIMS as well as supporting controls that should be implemented. These requirements are in alignment with the GDPR requirements and help to provide independent 3rd party validation to an organization's adherence to the GDPR.
How does the Court of Justice of the European Union's (CJEU) Schrems II decision to invalidate Privacy Shield affect InCountry?	With InCountry's data residency's platform now available in every EU/EEA country, we've made it easy for our customers to leverage global applications while ensuring regulated data stays within the EU with no access from the United States. Customers can rest assured that their data is secure and compliant with local regulations.
Can other customers see my data? Or is the data separate?	No, other customers will not be able to see each other's data. InCountry offers a separated and physically fully isolated architecture for each customer.
How is customer access organized within the InCountry platform?	InCountry helps to ensure that safeguards are in place to enforce authentication, authorization, and other identity and access management functions. Multifactor authentication is superior to standard password authentication because it requires another layer to authenticate the user. At InCountry, multifactor authentication is an absolute must for InCountry administrators.
Does you conduct network penetration tests?	Penetration tests are performed to provide assurance that administrative systems are secured and to increase the difficulty for malicious programs or users to exploit those systems. InCountry schedules international penetration tests for administrative systems by gathering a list of those systems and plan dates to execute internal penetration tests.
What is your security and compliance strategy?	The customer owns their data. In the case of contract termination, InCountry will retain the customer data as agreed in the contract for data retrieval purposes or migration. Post data retention interval InCountry deletes customer data on the InCountry platform and all relevant storage infrastructure. InCountry deletes the logical volumes, which will cause the storage device to re-use the storage space and overwrite the customer data.

sales@incountry.com
Phone:+1-415-323-0322
InCountry.com

InCountry -- FAQ

Security and Compliance

Question	Response
How do I connect to the InCountry platform?	Customers can connect using either a site-to-site IPSec VPN connection or via TLS 1.2 connections.
Will InCountry Support be offered with the platform?	InCountry's enterprise solutions include standard support. There is no additional fees.
How can I get started?	You can get started today by contacting your InCountry Sales team at sales@incountry.com.

sales@incountry.com
Phone:+1-415-323-0322
InCountry.com