ComplianceDesktop®
ANTI-CORRUPTION COMPLIANCE PLATFORM

The Anti-Corruption Compliance Platform

DATA COLLECTION | RISK IDENTIFICATION | SCREENING | INTEGRITY DUE DILIGENCE CERTIFICATIONS | GIFTS, TRAVEL AND ENTERTAINMENT TRACKING

SECURITY AND DATA PROTECTION

The ComplianceDesktop® | Anti-Corruption Compliance Platform was built and maintained with security in mind. To ensure that the platform remains secure, we choose follow and be certified in the global standard for information security: ISO 27001. We are also committed to transparency and protecting your sensitive information with our security and data privacy controls.

We leverage Amazon Web Services (AWS) to manage the physical, networking and hosting security of the ComplianceDesktop® solution, while we handle the application security

- **Industry-recognised certifications and audits**
- **World-class data centres**
- **Self-certify compliance with Safe Harbor and TRUSTe**

PHYSICAL SECURITY

Industry-recognised certifications and audits

AWS is a secure, durable technology platform with industry-recognised certifications and audits, including PCI DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 (formerly referred to as SAS 70 and SSAE 16) and SOC 2 audit reports. AWS services and data centres have multiple layers of operational and physical security to ensure the integrity and safety of your data.

World-class data centres

Amazon has many years' experience designing, constructing and operating large-scale data centres. AWS data centres are housed in nondescript facilities and critical locations, and have extensive setback and military-grade perimeter-control berms as well as other natural boundary protection. Physical access is strictly controlled at the perimeter and at building ingress points by professional security staff utilising video surveillance, state-of-the-art intrusion-detection systems and other electronic means. Authorised staff must pass two-factor authentication no fewer than three times to access AWS security data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorised staff.

Amazon only provides data-centre access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or AWS. All physical and electronic access to data centres by Amazon employees is logged and audited routinely.

For further details on AWS security, please refer to aws.amazon.com/security.

APPLICATION SECURITY

Application security refers to the features and measures that are built into the application to defend against threats, attacks and vulnerabilities. Many involve credentials requirements, encryption, limitation on sign-in attempts, and the use of roles and permissions to restrict access to certain data and documents.

Passwords

ComplianceDesktop® allows full integration with single sign-on (SSO) via SAML. This allows those enterprises using SSO to provide their users with seamless access to ComplianceDesktop®. It also lets system administrators manage authentication for ComplianceDesktop® and the rest of their corporate network through a SSO system.

Even without SSO, ComplianceDesktop®:

- requires users to possess a unique user ID and password to ensure only those who are authorised can access the system
- informs users of an error when they fail to enter valid credentials (user name and password), and a generic message prevents unauthorised users from acquiring information from sign-in errors
- obscures password characters on the login screen to avoid shoulder surfing
- restricts accounts after a certain number of unsuccessful login attempts
- has a timeout feature for idle sessions (including a pop-up warning to users before saving and then terminating the session).

Encryption

ComplianceDesktop® provides encryption of documents in transit via Secure Sockets Layer (SSL). The protocol allows applications to communicate across a network in a way designed to prevent eavesdropping and tampering. It also provides endpoint authentication and communications confidentiality over the internet, so that data sent from a client workstation to the ComplianceDesktop® is secure. All data and attachments are also encrypted.

Groups and permissions

ComplianceDesktop® uses groups and permissions to allow or restrict access to data. A number of groups can be created and privileges can be assigned on a per-application basis. You can also structure access based on geography, division, department or any number of variations. This ensures that data is accessible only on a least-privilege principle. Using groups to present users with the most relevant information and tools has the added benefit of making their jobs easier and more streamlined.

Backup

The Red Flag Group client databases are fully backed up by AWS.

Data Protection Principles according to European Commission Directives (95/46/EC)

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions (schedule 2 and 3) is met and the data subject has given his or her consent to the processing.
- Personal data shall be obtained only for one or more specific lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

Data protection and Safe Harbor

Concepts of data privacy differ among nations and regions, making it difficult to adopt privacy practices that satisfy all governments and their citizens. The European Union (EU) has developed eight principles for data protection, and each nation within the EU is required to incorporate these principles into their own data-protection acts.

The United States views privacy differently than the EU. There is no single or overarching inalienable right to privacy enshrined in United States law. Instead, different types of privacy rights have been established on a case-by-case basis by the United States Supreme Court through interpretation of various constitutional amendments. Many individual states also protect privacy and data to varying degrees.

Due to these differences, the United States has not incorporated the EU principles into federal law, which initially put the United States at a disadvantage when dealing with European nations and citizens. One particular provision of the EU regulations states that data may not leave the EU unless the receiving or hosting country ensures adequate protection for the data, equivalent to that of the EU. To help United States enterprises fulfil this adequate level of protection, the United States Department of Commerce, in consultation with the EU, created what is known as the Safe Harbor framework. Organisations can self-certify and publicly state that they comply with the Safe Harbor framework. Self-certification must be renewed annually, in writing, with the United States Department of Commerce. All organisations that have completed self-certification are listed on a public website at www.export.gov/safeharbor.

Update: In October 2015, the Court of Justice of the European Union ruled that the EU-US Safe Harbor regime was no longer a valid mechanism to legally transfer personal data from the EU to the US. The Red Flag Group has responded to this ruling by offering clients the opportunity to enter into Data Processing Addendums, which will incorporate the European Commission's Model Contract Clauses into the terms of their supply agreements. However, we maintain our commitment to the Safe Harbor principles, and intend on re-certifying when our registration falls due in anticipation of a new Safe Harbor regime being agreed in early 2016.

We self-certify compliance with

U.S. EU SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE

TRUSTe
EU SAFE HARBOR

AWS has already obtained Safe Harbor certification for their infrastructure and services. As The Red Flag Group serves global customers and ComplianceDesktop® may contain personal and sensitive information, we must, and do, comply with the EU principles via the Safe Harbor provisions. Our compliance is specified in our privacy policy and supported by our organisational practices. In addition to self-certification, The Red Flag Group has received

third-party verification of our privacy practices through TRUSTe, a leading internet privacy services provider (www.truste.com). The TRUSTe badge on our website lends extra assurance that The Red Flag Group takes privacy issues seriously and has attained Safe Harbor status. It also provides our customers with an unbiased mediator if there is a complaint regarding our privacy practices. The table below describes the seven Safe Harbor Principles and how The Red Flag Group complies with them.

How The Red Flag Group complies with the seven Safe Harbor Principles

Safe Harbor Principle	The Red Flag Group compliance
Notice: Organisations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organisation with any enquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organisation offers for limiting its use and disclosure.	The Red Flag Group discloses data collection purposes and practices in our privacy policy, available on our website at www.redflaggroup.com/privacy-policy.
Choice: Organisations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorised by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorised subsequently by the individual.	The Red Flag Group clearly states in its privacy policy whether, and under which circumstances, personal information may be disclosed, and provides the opportunity to opt out of this disclosure.
Onward transfer (transfers to third parties): To disclose information to a third party, organisations must apply the notice and choice principles. Where an organisation wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor Principles or is subject to the Directive or another adequacy finding. As an alternative, the organisation can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.	Onward transfer is discussed in the privacy policy, but The Red Flag Group specifically does not share, sell, rent or trade personally-identifiable information with third parties other than as disclosed within the privacy policy.
Access: Individuals must have access to the personal information that an organisation holds about them, and must be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.	Any individual wishing to review or update personally-identifiable information may contact us and we will facilitate that process.

Safe Harbor Principle	The Red Flag Group compliance
Security: Organisations must take reasonable precautions to protect personal information from loss, misuse and unauthorised access, disclosure, alteration and destruction.	The Red Flag Group takes reasonable technical, administrative and physical steps to protect against unauthorised access to and disclosure of personally-identifiable information. For example, only certain staff members have access to the service and are not allowed to view individual customer documents. Our support team may not login to customer's accounts without specific permission from the customer.
Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organisation should take reasonable steps to ensure the data is reliable for its intended use, accurate, complete and current.	As stated in our privacy policy, The Red Flag Group will not process personally-identifiable information in any way that is incompatible or inconsistent with the purpose for which the information was collected. We take all reasonable measures to ensure that the information is reliable for its intended use, and is accurate, complete and current.
Enforcement: In order to ensure compliance with the Safe Harbor Principles, there must be: • readily-available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide • procedures for verifying that the commitments companies make to adhere to the Safe Harbor Principles have been implemented • obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organisation. Organisations that fail to provide annual self-certification letters will no longer appear in the list of participants and Safe Harbor benefits will no longer be assured.	The Red Flag Group has committed to voluntarily and periodically reviewing our privacy and security practices to verify that we are meeting our obligations. As mentioned, we have been granted a TRUSTe seal of approval that we comply with Safe Harbor Principles. TRUSTe is an independent organisation that specialises in internet privacy. Any customer's concerns or complaints around data privacy issues may be registered with TRUSTe. We will cooperate with TRUSTe on any subsequent investigation and will abide by their resolution.

CONCLUSION

Moving data offsite to a third-party provider is a momentous decision for any corporation. The Red Flag Group understands our customers' security concerns and actively addresses them by:

- using AWS as our provider because of its commitment to maintaining military-grade security of its facilities
- integrating with SSO to enable individual organisations to extend their own password and security structure to their ComplianceDesktop® implementation
- using SSL for encrypted transmission of documents
- using groups and permissions to restrict access to the function levels
- regularly backing up customer data and the massive redundancy in the AWS infrastructure
- adhering to the principles of data protection via the Safe Harbor framework and TRUSTe verification.

About

The Red Flag Group is a global integrity and compliance risk firm. We apply our unique set of advice, technology and business intelligence applications to manage the integrity and compliance risks of our customers. We have a proven methodology that we use to help companies manage these risks. For more information, please visit www.redflaggroup.com.