Amazon data protection policy

Visualsoft

Amazon data protection policy

This policy is written to ensure that Visualsoft are compliant for the Amazon policies below and governs the collection, processing, storage, usage and disposal of Amazon data obtained for the use of clients from the Amazon Marketplace Web Service APIs:

Acceptable Use Policy (effective January 1, 2021)
Data Protection Policy (effective January 1, 2021)

General security requirements

Consistent with industry-leading security standards and other requirements specified by Amazon based on the classification and sensitivity of Amazon Information, Visualsoft maintains physical, administrative, and technical safeguards, and other security measures (i) to maintain the security and confidentiality of Amazon Information accessed, collected, used, stored, or transmitted by Visualsoft, and (ii) to protect that information from known or reasonably anticipated threats or hazards to its security and integrity, accidental loss, alteration, disclosure, and all other unlawful forms of processing. Without limitation, Visualsoft complies with the following requirements:

Network protection

All Visualsoft servers implement network protection controls including network firewalls. Public access is restricted to authorised users.

Access management

Access to Amazon information is strictly limited to users who require access in order to perform specific required tasks, and access is limited where possible to only required data. All users are unique with no shared logins and 2 Factor Authentication is in operation. Access is logged and monitored. Employees must request access and provide a reason when accessing Amazon data. Access can be revoked at any time if required and is reviewed regularly. Upon leaving the company, Access Permissions are revoked immediately. No Amazon data is allowed to be stored on removable devices, other than anonymised data such as overall sales figures. No PII is ever downloaded onto devices. Where suspicious activity is detected, such as multiple failed logins or large numbers of requests, account permissions will be revoked immediately and investigated by Systems Administrators.

Encryption in transit

All data in transit is encrypted using HTTPS on Visualsoft systems as data traverses the network. There are no instances of data in transit not being encrypted, even unused.

Incident response plan

Visualsoft has an incident response plan to deal with an interruption to, or degradation of, a service or component/configuration item, that has or may have an impact upon Visualsoft, it's clients or it's ability to provide a service to it's clients. Impact and urgency are both assessed according to set criteria then according to these rules, the appropriate employees will be informed. This may be a support ticket that is resolved, or else escalated. If the incident is deemed high priority, a special incident is declared in which case one or more of the following would have to be informed: Technical Support Team Leader, Customer Support Manager, Head of Service Delivery and Any Chief. Roles and responsibilities will be defined within the incident response team according to the exact requirements of the nature of the incident. All documentation relating to the incident is stored in the form of support tickets and meeting minutes to be made available later if requested by Amazon. We have separate policies for a Platform Wide Incident and a Security Data Breach. In the case of a data breach of sensitive data, including Amazon data, The Chief Technical Officer and Chief Executive Officer will be notified and the incident response team will be convened to triage, identify mitigations and remediation and to develop a communication plan to notify stakeholders. In the case of any Amazon data breach this includes emailing 3p-security@amazon.com within 24 hours of discovery. No regulatory authority, nor any customers will be notified, on behalf of Amazon unless Amazon specifically requests in writing that the Developer do so. These incident response plans are reviewed every 6 months, or in the case of major platform changes, sooner.

Request for Deletion or Return

Within 72 hours of Amazon's request, Visualsoft will permanently and securely delete (in accordance with NIST 800-88 industry-standard sanitization processes) or return Amazon Information in accordance with Amazon's notice requiring deletion and/or return. Visualsoft will also permanently and securely delete all live (online or network accessible) instances of Amazon Information within 90 days after Amazon's notice. If requested by Amazon, Visualsoft will certify in writing that all Amazon Information has been securely destroyed.

Additional security requirements specific to personally identifiable information

The following additional Security Requirements are met for all Personally Identifiable Information ("PII"), including instances where PII is combined with non PII:

Data retention and recovery

Amazon PII is stored by Visualsoft on privately hosted Database Servers for the sole purpose of facilitating the management of client orders. Amazon PII is removed from Visualsoft's databases no more than 30 days after the fulfillment of an order. Cancelled orders may have PII removed earlier. There is no Amazon PII stored in logs or other files.

Data governance

Visualsoft has an asset management policy defining how the software and physical assets are kept in an inventory and how this is updated as assets are reassigned or added. It also specifies procedures for data cleansing as assets are re-assigned or removed from the inventory. This is reviewed every 6 months and a full asset inventory is performed. Visualsoft also has a publicly available privacy policy stating our compliance to all applicable data privacy regulations.

Encryption and storage

All PII is encrypted at rest using industry standard AES-256 encryption. No PII is allowed to be stored in external media or unsecured Cloud applications. All cryptographic materials (encryption/decryption keys) and cryptographic capabilities used for encryption of PII at rest are only accessible to the Visualsoft system processes and services on our privately hosted cloud servers. Visualsoft have a procedure for securely disposing of printed documents with the 3rd party “Shred-it”, though this is explicitly prohibited by Visualsoft policy.

Least privilege principle

Access is provided to developers and other employees on a need to know basis using fine grained access controls to assign specific roles to minimise access based on the need to perform duties.

Logging and monitoring

Admin panel logging including access logs and authorization attempts are logged and stored for 12 months. No PII is ever logged anywhere on Visualsoft Systems. Code changes are logged to specific users. API logs are stored in databases on our privately hosted cloud servers, again not containing PII. Unauthorized access or unexpected request rates are flagged and suspicious activity is monitored by system administrators who will instigate an investigation as detailed in the Visualsoft Incident Response Plan.

Audit

Visualsoft will provide Amazon with all records if requested that demonstrate compliance with the Acceptable Use Policy, Data Protection Policy, and Amazon Marketplace Developer Agreement during the period of our agreement with Amazon and for 12 months thereafter. Visualsoft will also cooperate fully with any auditor assigned by Amazon and allow them to inspect the books, records, facilities, operations, and security of all systems that are involved with Visualsoft's application in the retrieval, storage, or processing of Amazon Information. Any breaches, failures or deficiencies flagged as part of any audit will be rectified by Visualsoft at our expense within the agreed timeframe.

www.visualsoft.co.uk

Teesside HQ
Visualsoft House
Prince's Wharf
Stockton-on-Tees
TS17 6QY

Visualsoft