Security Questionnaire version 1.22

How does AudienceProject collect data and produce its reports and segments?	When customers implement our AudienceProject service, they have full control over where data is collected and sent to AudienceProjects platform. The customer is in charge of creating tracking-scripts and pixels and deploying those data collection services on the inventory that the customer want to track. Data is then pushed from the customers selected endpoints and sent into AudienceProjects platform. Web based scripts and tracking pixels in collect and store the standardised apache web log file format as default. Our customers then can visit www.audiencereport.com or www.userreport.com in order to decide which data to include in any reports and to generate project specific reports either through our web-interface or the provided API.	Data collection
Where are AudienceProjects data Centers located?	AudienceProject serves customers globally. We currently operate from data-centers located in Ireland, Germany and the United States through Amazon web services.	Data Center
What security features does AudienceProject's data centers provide?	SECURE DESIGN SITE SELECTION Prior to choosing a location, AWS performs initial environmental and geographic assessments. Data center locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our Availability Zones are built to be independent and physically separated from one another. REDUNDANCY Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AVAILABILITY AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that	Data Center

	automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. CAPACITY PLANNING AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage. BUSINESS CONTINUITY & DISASTER RECOVERY BUSINESS CONTINUITY PLAN The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement. PANDEMIC RESPONSE AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies. PHYSICAL ACCESS EMPLOYEE DATA CENTER ACCESS AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. THIRD-PARTY DATA CENTER ACCESS Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are	

	time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff. AWS GOVCLOUD DATA CENTER ACCESS Physical access to data centers in the GovCloud (US) region is restricted to employees who have been validated as being US citizens. MONITORING & LOGGING DATA CENTER ACCESS REVIEW Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon. DATA CENTER ACCESS LOGS Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. DATA CENTER ACCESS MONITORING We monitor our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses. SURVEILLANCE & DETECTION CCTV Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements. DATA CENTER ENTRY POINTS Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open. INTRUSION DETECTION Electronic intrusion detection systems are installed within the data layer to monitor, detect, and	

	automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response. DEVICE MANAGEMENT ASSET MANAGEMENT AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution. MEDIA DESTRUCTION Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned. OPERATIONAL SUPPORT SYSTEMS POWER Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility. CLIMATE AND TEMPERATURE AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels. FIRE DETECTION AND SUPPRESSION AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems. LEAKAGE DETECTION In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any	

	additional water damage. INFRASTRUCTURE MAINTENANCE EQUIPMENT MAINTENANCE AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule. ENVIRONMENT MANAGEMENT AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment. GOVERNANCE & RISK ONGOING DATA CENTER RISK MANAGEMENT The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration. THIRD-PARTY SECURITY ATTESTATION Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.	
Does AudienceProject conduct regular internal audits?	AudienceProject run ongoing assessments by performing regular, automated, vulnerability scans on our external and internal networks. In AudienceProject we operate with a mix of manual and automated audits. We have two different automated audit services running continuously: Guard-duty and Inspector. Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on our network. Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Inspector produces a detailed list of security findings prioritised by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via our Inspector console or API.	Security Audits

	GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorised behaviour to help us protect our network accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorised deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers. GuardDuty identifies suspected attackers through integrated threat intelligence feeds and uses machine learning to detect anomalies in account and workload activity. When a potential threat is detected, the service delivers a detailed security alert to our GuardDuty console. Further, security review is an integral part of our development lifecycle, incorporated into our design, implementation, and test processes.	
What are AudienceProject's corporate password requirements?	We use Google Auth for a single sign on platform in combination with AWS Cognito. Those two services controls our access to the various applications that AudienceProject uses. Multi factor authentication is mandatory in order to gain access to our internal services system. With regards to the password policy specifically,they are set as follows: (a) passwords must be a minimum of 10 characters; (b) they must contain some lower case letters, and they cannot contain part of the username; and (c) users are locked out after 4 failed login attempts and disabled automatically if suspicious device or IP activity is detected .	Access controls
How are customer logins and passwords protected?	AudienceProject offers a unique Single Sign On solution across its entire Audience platform. The service is based on AWS Cognito. Social and enterprise identity federation With Single Sign On, your users can sign-in through social identity providers such as Google, Facebook, and Amazon, and through enterprise identity providers such as Microsoft Active Directory using SAML. Access control for AP resources Single Sign On provides solutions to control access to AP resources from your account. You can define roles and map users to different roles so your users can access only the resources that are authorized for each user. Standards-based authentication Single Sign On uses common identity management standards including OpenID Connect, OAuth 2.0, and SAML 2.0. Adaptive authentication Using advanced security features for Single Sign On to add adaptive authentication to your accounts helps protect your applications' user accounts and user experience. When Single Sign On detects unusual sign-in activity, such as sign-in attempts from new locations and devices, it assigns a risk score to the activity and lets prompt users for additional verification or block the sign-in request. Users can verify their identities	Access controls

	using SMS or a Time-based One-time Password (TOTP) generator, such as Google Authenticator. Protection from compromised credentials Advanced security features forSingle Sign On helps protect your application users from unauthorized access to their accounts using compromised credentials. WhenSingle Sign On detects users have entered credentials that have been compromised elsewhere, it prompts them to change their password. Supports Multiple Compliance Programs Single Sign On helps you meet multiple security and compliance requirements, including those for highly regulated organizations such as healthcare companies and merchants. Single Sign On is HIPAA eligible and PCI DSS, SOC, and ISO/IEC 27001, ISO/EIC 27017, ISO/EIC 27018, and ISO 9001 compliant.	
Does AudienceProject use encryption?	AudienceProject operates through Amazon Web Services and uses encryption in transit and encryption at rest for all relevant Amazon Web Services services used. Moreover, internal emails are TLS encrypted.	