Appendix C.2 – Security of processing

Technical security	Description
Antivirus	All customer data is only accessible via a cloud platform. The cloud solution with WP Engine, Microsoft, AWS, and Google Cloud contains a prominent level of security of the server, storage and network which supports viruses and malicious code detection. Amplitude leverages threat detection tools to monitor and alert Amplitude to suspicious activities, potential malware, viruses, and/or malicious computer code
Firewall	All customer data is hosted on the cloud. Each cloud provider specifies their own security system protection in appendix B. 1.
Network segmentation	Network segmentation is not relevant for the local network at Pleaz because of the company's choice of a cloud solution.
System monitoring	Pleaz' has access to system monitoring via the different cloud providers. The monitoring we do today is optimized for tracking technical performance and usage.
Encryption by transmission	Data transmission from the customer to Pleaz' customer platform is encrypted with TLS 1.2. The WP Engine cloud solution supports AES-256 encryption of the Pleaz platform. Microsoft Could makes encryption of data at rest available using AES-256, the data is also always secured in transit by using HTTPS. Google Cloud makes HTTPS encryption (also referred to as SSL or TLS connection) available and allows for encryption of data in transit. Google Cloud also makes encryption of data at rest available using AES-256. Amplitude utilizes the AWS platform and uses FIPS 140-2 and/or NIST SP800-52 encryption standards Axiom utilizes the AWS platform and uses AES-256 encryption and TLS to secure network traffic
Logging	Microsoft Cloud, Google Cloud, WP engine have their own logging system. Anomalies are investigated and prioritized. Pleaz also use Axiom for logging. All logs and metrics are encrypted, stored separately from customers data, and contain only device information for incident investigations.

	WP Engine will continuously review logs for the operation of the entire cloud platform, while logs with customer data, specific for Pleaz, is observed internally by the company.
Backup	All customer data is supported with backup systems. All backups are encrypted via SSL in transit and encrypted at rest
Test environment	Pleaz have their own local test environment for software development and two different online environments for testing purposes. Production data is not used for software development and/or testing. All data used in the test environment is created for this purpose only and does not include personal data.
Vulnerability testing	The cloud solution supports test of system vulnerabilities. Sub processors conduct regular security audits and penetration tests to identify and address vulnerabilities.
Updates and patches	Security patches are installed immediately. Updates patches are installed after being carefully vetted.
User access and rights	Pleaz has implemented a minimum access approach, so that all employees start with the essentials and get extended access depending on their needs.
Two-factor login	A two-factor authentication of access to customer data has been implemented to the Microsoft cloud solutions. It is possible to access changes in administration rights and logs for failed login attempts via the cloud solution.

Physical security	Description
Premises	Access to the data processor's offices requires a key or an appointment at the front door. After business hours, the offices will be locked separately. Pleaz has no physical documents containing sensitive data.