UHY LLP
Certified Public Accountants

Liquid Web™

GDPR

Liquid Web, LLC

Co-Location, Web Hosting, and Network Infrastructure Services

Report on Management's Assertion on an Information Security Management System to meet General Data Protection Regulation Objectives

UHY LLP
www.uhy-us.com

The next level of service

Table of Contents

Section 1:

Independent Service Auditor's Report

UHY LLP
Certified Public Accountants

To the Management of:
Liquid Web, LLC
2703 Ena Dr.
Lansing, MI 48917

Scope

We have examined management of Liquid Web, LLC's ("Liquid Web") assertion that management has developed and implemented an information security management system over Liquid Web's co-location, web hosting, and network infrastructure services provided to user entities related to the General Data Protection Regulation ("GDPR") of the European Union ("EU") and that the controls were suitably designed, implemented, and operated effectively throughout the period November 1, 2021 to October 31, 2022.

Liquid Web uses third-party service providers to provide physical security, internet connection, and environmental controls for the Arizona and Netherlands facilities. The information security management system was designed with the assumption that the third-party service providers have controls in place that are suitably designed and operating effectively, along with controls at Liquid Web, to achieve Liquid Web's service commitments. The controls at the third-party service providers are not in-scope for management's assertion. Our examination did not include the services provided by the third-party service providers, and we have not evaluated the suitability of the design or operating effectiveness of the third-party service providers' controls.

The information included in Section 5, "Other Information Provided by Liquid Web, LLC That is Not Covered by the Independent Accountant's Report", is presented by Liquid Web's management to provide additional information and is not a part of Liquid Web's information security management system for co-location, web hosting, and network infrastructure services system made available to user entities during the period November 1, 2021 to October 31, 2022. Information about Liquid Web's management response to exceptions identified in the report has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Service organization and service auditor responsibilities

Liquid Web's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent limitations

The information security management system is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable General Data Protection Regulations. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion Liquid Web's assertion that management has developed and implemented an information security management system over Liquid Web's co-location, web hosting, and network infrastructure services provided to user entities related to the GDPR of the EU and that the controls were suitably designed, implemented, and operated effectively throughout the period November 1, 2021 to October 31, 2022, is fairly stated, in all material respects.

Restricted use

This report is intended solely for the information and use of management of Liquid Web and user entities of the co-location, web hosting, and network infrastructure services and is not intended to be and should not be used by anyone other than these specified parties.

Farmington Hills, MI
July 11, 2023

Section 2:

Liquid Web, LLC Management's Assertion

Management of Liquid Web, LLC's Assertion:

We have developed and implemented an information security management system over Liquid Web, LLC's ("Liquid Web") co-location, web hosting, and network infrastructure services provided to user entities relevant to the General Data Protection Regulation ("GDPR") of the European Union ("EU").

Compliance with GDPR for user entities' environments is the responsibility of the user entity. User entities are responsible for designing and implementing internal controls, including monitoring controls at service providers, to address their compliance requirements. Liquid Web provides services that may impact or be necessary to support the user entities' compliance initiatives. As a result, the information security management system was developed to define Liquid Web's services commitments related to GDPR.

The information security management system was developed to identify relevant areas where Liquid Web's services provided to user entities may impact or be necessary to support the user entities' internal control related to GDPR and controls were implemented to address the identified areas to the co-location, web hosting, and network infrastructure services provided by Liquid Web. The controls included in the system are limited to those Liquid Web believes are likely to be relevant to user entities' internal controls related to GDPR.

Liquid Web uses third-party service providers to provide physical security, internet connection, and environmental controls for the Arizona and Netherlands facilities. The information security management system was designed with the assumption that the third-party service providers have controls in place that are suitably designed and operating effectively, along with controls at Liquid Web, to achieve Liquid Web's service commitments. The controls at the third-party service providers are not in-scope for management's assertion.

We confirm, to the best of our knowledge and belief, that—

1) The information security management system over Liquid Web's co-location, web hosting, and network infrastructure services system was designed and implemented throughout the period November 1, 2021 to October 31, 2022 in order to meet the objectives of Liquid Web's services commitments related to GDPR.
2) The controls included in the information security management system were suitably designed throughout the period November 1, 2021 to October 31, 2022 to provide reasonable assurance that Liquid Web's service commitments related to GDPR would be achieved if the controls operated effectively during the period.
3) The controls included in the information security management system operated effectively throughout the period November 1, 2021 to October 31, 2022 to provide reasonable assurance that Liquid Web's service commitments related to GDPR were achieved.

Nick Campbell
Senior Director of Security and Architecture
Liquid Web, LLC

Section 3:

Independent Accountant's GDPR Testing Approach and Key Findings

TESTING APPROACH

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Our examination was conducted using the controls mapping provided by Liquid Web, LLC and the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Liquid Web management designed and implemented controls pertinent to GDPR based on the in-scope services. The information security management system includes only the controls developed and implemented by Liquid Web to support management's services commitments to user entities related to GDPR. The information security management system includes a mapping of the pertinent controls to the applicable GDPR. This mapping includes only Liquid Web's controls and does not include the user entity controls that are necessary to meet the GDPR.

Our tests of the control environment included the following procedures, to the extent we considered necessary: (a) a review of the organization's organizational structure, including the segregation of functional responsibilities, policy statements, accounting and processing manuals, personnel policies and the internal audit's policies; (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; and (c) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of our testing of their controls to support our conclusions on the achievement of selected control objectives.

Our examination of the suitability of design and operational effectiveness of controls included the testing necessary, based upon our judgment, to evaluate whether adherence with those controls was sufficient to provide reasonable, but not absolute, assurance that the specified control objectives included below were achieved throughout the stated period.

KEY FINDINGS

A number of GDPR requirements were determined to be not applicable ("N/A") to Liquid Web, given their operating structure and the nature of the services provided. These areas are discussed in this section.

The relevant GDPR Articles included Articles 28, 29, 31, 32, 33, 35, 37, 40, and 41. The other Articles in the Regulation were determined to be not applicable due to the Articles addressing requirements specifically for data controllers, the individual unions, or processing activities not provided by Liquid Web. Key processor requirements that were not applicable due to the nature of the services provided by Liquid Web include the following:

- Transfer of personal data to third countries or international organization
    - Liquid Web transfers no client data from a data center outside of the country that the data center is located in as part of their standard services. All customer data for US and Netherlands customers stays within the United States and the Netherlands respectfully, unless the customer initiates an external transfer.
- Data Encryption
    - Liquid Web does not provide data encryption services to customers. Customers are solely responsible for the encryption of their data within the Liquid Web environment.

- Access to personal data within customer environments
    - Liquid Web does not have access to customer applications of data. As such, Liquid Web does not have access to personal data of the customer's data subjects.
- Communication of personal data breach to the data subject
    - Liquid Web does not have access to customer applications or data. As such, Liquid Web does not have to ability to determine if a data subject's information has been breached. Identification and notification of data breaches to data subjects is solely the responsibility of the customers.

Section 4:

GDPR Requirements, Related Controls, and Test of Controls

Article 28 - Processor				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
28.1	The processor shall not engage another processor without prior specific or general written authorization of the controller.	Each service offering has established terms of service which outline the services and associated boundaries for external users. Terms of Service and Service Level Agreements are available and communicated on the public website for external users.	Inspected established Terms of Service and Service Level Agreements for the in-scope services to verify that they outlined the services and associated boundaries for external users. Inspected the organization's public website to verify that Terms of Service and Service Level Agreements are available and communicated on the public website for external users.	No exceptions noted.
		Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.	Inspected the GDPR data processing addendum to verify that data processing agreements outlined the controller and processor responsibilities.	No exceptions noted.
28.2	Processing by a processor shall be governed by a contract or other legal act under Union or Member State law. That contract or other legal act shall stipulate the requirements outlined in Article 28 paragraph 3.	Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.	Inspected the GDPR data processing addendum to verify that data processing agreements outlined the controller and processor responsibilities.	No exceptions noted.
		Each service offering has established terms of service which outline the services and associated boundaries for external users. Terms of Service and Service Level Agreements are available and communicated on the public website for external users.	Inspected established Terms of Service and Service Level Agreements for the in-scope services to verify that they outlined the services and associated boundaries for external users. Inspected the organization's public website to verify that Terms of Service and Service Level Agreements are available and communicated on the public website for external users.	No exceptions noted.
		Security and availability commitments made to external users are communicated within the Terms of Service, which are available and communicated on the public website for external users.	Inspected established Terms of Service and Service Level Agreements for the in-scope services to verify that they outlined the security and availability commitments made to external users. Inspected the organization's public website to verify that Terms of Service are available and communicated on the public website for external users.	No exceptions noted.

Article 28 – Processor				
GDPR Article		Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
28.3	The processor adheres to an approved code of conduct.	Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.	Inspected the GDPR data processing addendum to verify that data processing agreements outlined the controller and processor responsibilities.	No exceptions noted.
		Employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	Inspected signed employee handbook acknowledgments for a sample of new hires to verify that employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	No exceptions noted.

Article 29 - Processing under the authority of the controller or processor				
GDPR Article		Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
29.1	The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.	Inspected the GDPR data processing addendum to verify that data processing agreements outlined the controller and processor responsibilities.	No exceptions noted.
		Each service offering has established terms of service which outline the services and associated boundaries for external users. Terms of Service and Service Level Agreements are available and communicated on the public website for external users.	Inspected established Terms of Service and Service Level Agreements for the in-scope services to verify that they outlined the services and associated boundaries for external users. Inspected the organization's public website to verify that Terms of Service and Service Level Agreements are available and communicated on the public website for external users.	No exceptions noted.

Article 31 - Cooperation with the supervisory authority				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
31.1	The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.	Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.	Inspected the GDPR data processing addendum to verify that data processing agreements outlined the controller and processor responsibilities.	No exceptions noted.
		A formal Incident Response Plan is in place that documents the process for identification, evaluation, response, and resolution. Additionally, the plan includes procedures for notifying the appropriate personnel and customers.	Inspected the Incident Management Plan to verify that a formal Incident Response Plan is in place that documents the process for identification, evaluation, response, resolution, and notification procedures.	No exceptions noted.

Article 32 - Security of processing				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
32.1	Personal data is secured through the use of pseudonymisation and encryption.	This Article is not applicable to the organization. Securing personal data through the use of pseudonymisation and encryption is the responsibility of the organization's customers.		
32.2	The processor ensures the ongoing confidentiality, integrity, availability and resilience of processing systems and services.	Quarterly external network assessments are performed to identify and address vulnerabilities and changes in the environment that may impact the security and availability of the system. The results of the assessments are communicated to IT management in a timely manner for review. Remediation efforts of issues found are documented by IT management.	Inspected completed external vulnerability scans and remediation documentation for the quarterly scans conducted during the attestation period to verify that quarterly external vulnerability scans were conducted, vulnerabilities were remediated, and results were communicated to IT management timely.	No exceptions noted.
		The organization uses an issue tracking system to record and monitor security and availability issues through resolution. Unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.	Inspected the issue tracking system to verify that the organization uses an issue tracking system to record and monitor security and availability issues through resolution. Inspected example issue tickets to verify that unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.	No exceptions noted.

Article 32 - Security of processing				
GDPR Article		Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
		Network monitoring tools are utilized to monitor network operations and provide real-time information on system performance and outages.	Inspected the network monitoring tools utilized by the organization and example alerts to verify that tools were used to monitor network operations and provide real-time information on system performance and outages.	No exceptions noted.
		Future capacity needs are tracked by IT management as a part of inventory management.	Inspected inventory management documentation to verify that future capacity needs are tracked by IT management as a part of inventory management.	No exceptions noted.
		Network authentication is controlled via redundant authentication servers. Access to the servers is restricted to authorized administrators.	Inspected configurations showing the redundant authentication servers to verify that network authentication is controlled via redundant authentication servers. Inspected user access groups and permissions to verify that authentication servers are controlled by the network engineering and system operations groups.	No exceptions noted.
		Encryption keys are utilized for authenticating to the organization's network. Encryption keys are generated randomly via an automated script.	Inspected authentication server encryption settings to verify that encryption keys were used for authentication to the network. Inspected the key generation script to verify that an automated script was used to generate authentication server encryption keys.	No exceptions noted.
		A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall interface configurations to verify that a firewall system is in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		An Intrusion Prevention System (IPS) is in place and sends alerts for high and critical severity vulnerabilities.	Inspected IPS settings and alert examples to verify that an IPS system was in place and sends alerts for high and critical severity vulnerabilities.	No exceptions noted.

Article 32 - Security of processing				
GDPR Article		Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
		Malware protection software is installed on all systems commonly affected by malicious software. Malware protection software is configured to update every 60 minutes and to run a weekly scan.	Inspected systems listings and malware protection software reports to verify that malware protection software is installed on all systems commonly affected by malicious software. Inspected malware protection software central management server settings to verify that malware protection software is configured to update every 60 minutes and to run a weekly scan.	No exceptions noted.
		Critical internal system and infrastructure code backups are run on at least a daily basis to enable recovery of data.	Inspected backup schedules to verify that critical internal system and infrastructure code backups are run on an at least daily basis to enable recovery of data.	No exceptions noted.
		Code backup systems generate backup logs and send alerts for failed backups to systems personnel for review.	Inspected backup log settings to verify that code backup systems generate backup logs. Inspected backup alert settings and examples to verify that code backup systems send alerts for failed backups to systems personnel for review,	No exceptions noted.
		Code backups are stored at a secondary data center to provide additional recoverability.	Inspected backup storage settings to verify that code backups are stored at a secondary data center to provide additional recoverability.	No exceptions noted.
		Critical internal system and infrastructure database backups run on an at least daily basis to enable recovery of data.	Inspected backup schedules to verify that critical internal system and infrastructure database backups run on an at least daily basis to enable recovery of data.	No exceptions noted.
		Database backup systems generate backup logs and send alerts for failed backups to systems personnel for review.	Inspected backup log settings to verify that database backup systems generate backup logs. Inspected backup alert settings and examples to verify that database backup systems send alerts for failed backups to systems personnel for review.	No exceptions noted.
		Database backups are stored at a secondary data center to provide additional recoverability.	Inspected backup storage settings to verify that database backups are stored at a secondary data center to provide additional recoverability.	No exceptions noted.
		Tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	Inspected tabletop system redundancy testing documentation to verify tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	No exceptions noted.

Article 32 - Security of processing				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
32.3	The processor has the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	Critical internal system and infrastructure code backups are run on at least a daily basis to enable recovery of data.	Inspected backup schedules to verify that critical internal system and infrastructure code backups are run on an at least daily basis to enable recovery of data.	No exceptions noted.
		Code backup systems generate backup logs and send alerts for failed backups to systems personnel for review.	Inspected backup log settings to verify that code backup systems generate backup logs. Inspected backup alert settings and examples to verify that code backup systems send alerts for failed backups to systems personnel for review,	No exceptions noted.
		Code backups are stored at a secondary data center to provide additional recoverability.	Inspected backup storage settings to verify that code backups are stored at a secondary data center to provide additional recoverability.	No exceptions noted.
32.4	The processor has a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.	Quarterly external network assessments are performed to identify and address vulnerabilities and changes in the environment that may impact the security and availability of the system. The results of the assessments are communicated to IT management in a timely manner for review. Remediation efforts of issues found are documented by IT management.	Inspected completed external vulnerability scans and remediation documentation for the quarterly scans conducted during the attestation period to verify that quarterly external vulnerability scans were conducted, vulnerabilities were remediated, and results were communicated to IT management timely.	No exceptions noted.
		Network monitoring tools are utilized to monitor network operations and provide real-time information on system performance and outages.	Inspected the network monitoring tools utilized by the organization and example alerts to verify that tools were used to monitor network operations and provide real-time information on system performance and outages.	No exceptions noted.
		An Intrusion Prevention System (IPS) is in place and sends alerts for high and critical severity vulnerabilities.	Inspected IPS settings and alert examples to verify that an IPS system was in place and sends alerts for high and critical severity vulnerabilities.	No exceptions noted.
		Code backup systems generate backup logs and send alerts for failed backups to systems personnel for review.	Inspected backup log settings to verify that code backup systems generate backup logs. Inspected backup alert settings and examples to verify that code backup systems send alerts for failed backups to systems personnel for review,	No exceptions noted.

Article 32 - Security of processing				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	Inspected tabletop system redundancy testing documentation to verify tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	No exceptions noted.
		A formal information security training program has been implemented. Employees receive security awareness training upon hire and annually thereafter.	Inspected the security training program to verify that a formal information security training program has been implemented. Inspected security awareness training documentation for the sample of new hires and current employees to verify that employees receive security awareness training upon hire and annually thereafter.	Exceptions noted.
		Exception Summary: For 4 of 45 (8.9%) sampled new hires, security awareness training was not completed timely. For 1 of 45 (2.2%) sampled new hires, security awareness training was not completed.		
32.5	The processor provides the appropriate level of security for the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.	User access for new employees is requested by the Human Resources/employee's manager through the Office IT department. The Office IT department assigns users to a group profile based on their role and department.	Inspected new hire provisioning documentation for a sample of new hires to verify that new user access is requested and approved by HR or the user's manager through the Office IT department. Inspected access permissions for a sample of new hires to verify that the Office IT Department assigned users to groups based on their department.	No exceptions noted.

Article 32 - Security of processing				
GDPR Article		Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
		Authorized users are identified and authenticated via a unique user ID and password. Access to hosting-related systems and infrastructure is further restricted via SSH and two-factor authentication. User IDs are unique and passwords are encrypted.	Inspected network authentication screens and example network security event logs to verify that all authorized users are identified and authenticated via a unique user ID and password. Inspected network authentication screens to verify that access to hosting related systems and infrastructure is further restricted via SSH and two-factor authentication. Inspected the user access listing to verify that User IDs are unique. Inspected the authentication system encryption settings to verity that passwords are encrypted.	No exceptions noted.
		Access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.	Inspected user access lists and permissions listing to verify that access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.	No exceptions noted.
		Administrative access to the in-scope (Firewalls, badge access system, IPS, network, authentication systems, VPN, etc.) systems is restricted to authorized system administration personnel.	Inspected user access listings to the in-scope systems to verify that the administrative access is restricted to authorized system administration personnel.	No exceptions noted.
		User access reviews are performed annually by the Department Heads to determine if access privileges are appropriate.	Inspected authentication system permissions audit documentation to verify that user access reviews are performed annually by the Department Heads to determine if access privileges are appropriate.	No exceptions noted.
		Surveillance cameras are in place to monitor and record activity throughout the facilities, work areas, and data centers. Surveillance video is retained for a minimum of 90 days.	Observed the surveillance cameras throughout the facilities, work areas, and data centers during onsite walkthrough to verify that cameras are in place to monitor and record activity. Observed historic surveillance video to verify that video is retained for a minimum of 90 days. Inspected surveillance cameras settings to verify that video is retained for a minimum of 90 days.	No exceptions noted.

Article 32 - Security of processing				
GDPR Article		Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
		Visitors are required to present a valid photo ID and are provided a visitor badge upon entry to the facilities. Visitors are escorted for the duration of their visit.	Observed the visitor check in process during onsite walkthroughs to verify that visitors are required to present a valid photo ID and are provided a visitor badge upon entry to the facilities. Observed visitors being escorted during onsite walkthroughs to verify that to verify that visitors are escorted for the duration of their visit.	No exceptions noted.
		Access to the data center is restricted to technical staff.	Observed the data access restrictions during onsite walkthroughs to verify that access is restricted to technical staff. Inspected badge system access listings to verify that access is restricted to technical staff.	No exceptions noted.
32.6	The processor adheres to an approved code of conduct.	Employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	Inspected signed employee handbook acknowledgments for a sample of new hires to verify that employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	No exceptions noted.
		Employees are required to acknowledge their understanding of their responsibility for adhering to the employee conduct standards and non-disclosure agreement upon hire.	Inspected employee handbook acknowledgments for a sample of new hires to verify that employees are required to acknowledge their understanding of their responsibility for adhering to the employee conduct standards upon hire. Inspected signed non-disclosure agreements for a sample of new hires to verify that employees are required to acknowledge their understanding of their responsibility for adhering to the non-disclosure agreement upon hire.	No exceptions noted.

Article 32 - Security of processing				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
32.7	The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.	Inspected the GDPR data processing addendum to verify that data processing agreements outlined the controller and processor responsibilities.	No exceptions noted.
		Each service offering has established terms of service which outline the services and associated boundaries for external users. Terms of Service and Service Level Agreements are available and communicated on the public website for external users.	Inspected established Terms of Service and Service Level Agreements for the in-scope services to verify that they outlined the services and associated boundaries for external users. Inspected the organization's public website to verify that Terms of Service and Service Level Agreements are available and communicated on the public website for external users.	No exceptions noted.

Article 33 - Notification of a personal data breach to the supervisory authority				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
33.1	The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.	Inspected the GDPR data processing addendum to verify that data processing agreements outlined the controller and processor responsibilities.	No exceptions noted.
		A formal Incident Response Plan is in place that documents the process for identification, evaluation, response, and resolution. Additionally, the plan includes procedures for notifying the appropriate personnel and customers.	Inspected the Incident Management Plan to verify that a formal Incident Response Plan is in place that documents the process for identification, evaluation, response, resolution, and notification procedures.	No exceptions noted.
		Status pages are in place and available to customers to communicate matters affecting customer services and the functioning of internal control.	Inspected the organization's status page to verify that status pages are in place and available to customers to communicate matters affecting customer services and the functioning of internal control.	No exceptions noted.

Article 35 - Data protection impact assessment				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
35.1	Data protection impact assessment are conducted periodically.	A formal risk assessment is performed on at least an annual basis that includes the following components: o Reviewing company operational, financial, reporting, and compliance objectives and identifying risks that threaten the achievement of those risks o Consideration of fraud risk to achievement of the objectives o The identification of changes to the internal, external, legal, regulatory, or technological environments that could impact the Company's system of internal control o Assessment of third-party risk o Assigning a risk rating and action plans for how the company will respond to the identified risks	Inspected risk assessment documentation to verify that an assessment was performed on an annual basis and included the stated components.	No exceptions noted.
		Tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	Inspected tabletop system redundancy testing documentation to verify tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	No exceptions noted.
35.2	Compliance with approved codes of conduct are taken into due account in assessing the impact of the processing operations.	Employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	Inspected signed employee handbook acknowledgments for a sample of new hires to verify that employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	No exceptions noted.
		Employees are required to acknowledge their understanding of their responsibility for adhering to the employee conduct standards and non-disclosure agreement upon hire.	Inspected employee handbook acknowledgments for a sample of new hires to verify that employees are required to acknowledge their understanding of their responsibility for adhering to the employee conduct standards upon hire. Inspected signed non-disclosure agreements for a sample of new hires to verify that employees are required to acknowledge their understanding of their responsibility for adhering to the non-disclosure agreement upon hire.	No exceptions noted.

Article 35 - Data protection impact assessment				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Employee evaluations are performed on at least an annual basis to evaluate and assess the conduct, performance, and skills of employees within the organization. Employee evaluations are used to determine compensation and development opportunities.	Inspected performance review documentation for a sample of current employees to verify that evaluations are performed on at least an annual basis to evaluate and assess the conduct, performance, and skills of employees within the company. Inquired of the HR Director to verify that evaluations are used to determine compensation.	Exception noted.
		Exception Summary: For 1 of 45 (2.2%) sampled employees, an annual performance evaluation was not conducted.		
		A corrective action policy in place that defines the procedures and sanctions to be taken in the event of non-compliance with the organization's standards of conduct and information security policies.	Inspected the employee handbook to verify that a corrective action policy in place that defined the procedures and sanctions to be taken in the event of non-compliance with the company's standards of conduct and information security policies.	No exceptions noted.

Article 37 - Designation of the data protection officer				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
37.1	The processor shall designate a data protection officer(s).	The organization has implemented a data protection and privacy team. The team meets regularly and are responsible for handling issues related to data protection and privacy.	Inquired of the Senior Director of Security & Architecture and Change and Compliance Manager to verify that the data protection and privacy team is responsible for handling issues related to data protection and privacy. Inspected examples of meeting invites to verify that the organization has implemented a data protection and privacy team that meets regularly.	No exceptions noted.

Article 40 - Codes of conduct				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
40.1	An approved code of conduct is in place an acknowledged by the processor's employees.	Employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	Inspected signed employee handbook acknowledgments for a sample of new hires to verify that employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	No exceptions noted.
		Employees are required to acknowledge their understanding of their responsibility for adhering to the employee conduct standards and non-disclosure agreement upon hire.	Inspected employee handbook acknowledgments for a sample of new hires to verify that employees are required to acknowledge their understanding of their responsibility for adhering to the employee conduct standards upon hire. Inspected signed non-disclosure agreements for a sample of new hires to verify that employees are required to acknowledge their understanding of their responsibility for adhering to the non-disclosure agreement upon hire.	No exceptions noted.

Article 41 - Monitoring of approved codes of conduct				
GDPR Article		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
41.1	The code of conduct is reviewed periodically, updated as necessary, and approved by management.	Employees are required to acknowledge their understanding of their responsibility for adhering to the employee conduct standards and non-disclosure agreement upon hire.	Inspected employee handbook acknowledgments for a sample of new hires to verify that employees are required to acknowledge their understanding of their responsibility for adhering to the employee conduct standards upon hire. Inspected signed non-disclosure agreements for a sample of new hires to verify that employees are required to acknowledge their understanding of their responsibility for adhering to the non-disclosure agreement upon hire.	No exceptions noted.

Section 5:

Other Information Provided by Liquid Web, LLC That Is Not Covered by the Independent Service Auditor's Report

OTHER INFORMATION PROVIDED BY LIQUID WEB, LLC

In addition to the information in Section 4, GDPR Requirements, Related Controls, and Test of Controls, the following additional information is being provided by Liquid Web's management as it may be relevant to the reader to obtain a better understanding of Liquid Web's exceptions. The following Management's Responses to the exceptions noted in Section 4 are not within the scope of this examination and have not been audited.

<table>
<tr><th colspan="3">Management's Responses to Exceptions Identified in Section 4</th></tr>
<tr><th>Criteria</th><th>Control Activity</th><th>Exception Summary</th></tr>
<tr><td>Article 32.4</td><td>A formal information security training program has been implemented. Employees receive security awareness training upon hire and annually thereafter.</td><td>For 4 of 45 (8.9%) sampled new hires, security awareness training was not completed timely.

For 1 of 45 (2.2%) sampled new hires, security awareness training was not completed.</td></tr>
<tr><td colspan="3">Management's Response:
Due to priority internal requirements a subset of employees did not complete their training in a timely manner, the training was completed at a later date. The gap in the process that allowed the new hire to miss taking training has been resolved.</td></tr>
<tr><th>Criteria</th><th>Control Activity</th><th>Exception Summary</th></tr>
<tr><td>Article 35.2</td><td>Employee evaluations are performed on at least an annual basis to evaluate and assess the conduct, performance, and skills of employees within the organization. Employee evaluations are used to determine compensation and development opportunities.</td><td>For 1 of 45 (2.2%) sampled employees, an annual performance evaluation was not conducted.</td></tr>
<tr><td colspan="3">Management's Response:
The employee's evaluation was conducted, but proper documentation was not completed. The process has been updated to ensure documentation is kept going forward.</td></tr>
</table>