Liquid Web™

INDEPENDENT ACCOUNTANT'S REPORT

LIQUID WEB, LLC

Report on Management's Assertion of Controls in Place Addressing General Data Protection Regulations

As of May 15, 2018

UHY LLP
Certified Public Accountants

LIQUID WEB, LLC

Report on Management's Assertion of Controls in Place Addressing General Data Protection Regulations

TABLE OF CONTENTS

UHY LLP
Certified Public Accountants

I. INDEPENDENT SERVICE PRACTITIONER'S REPORT

To the Management of Liquid Web, LLC:

Scope

We have examined management's assertion that Liquid Web, LLC ("Liquid Web") has controls in place that address the General Data Protection Regulation ("GDPR") of the European Union ("EU") as of May 15, 2018. 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 American Institute of Certified Public Accountants. 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.

Opinion

In our opinion, management's assertion that Liquid Web has controls in place that address the General Data Protection Regulation ("GDPR") of the European Union ("EU") as of May 15, 2018 is fairly stated, in all material respects, based on applicable General Data Protection Regulations.

Other matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Restricted use

This report is intended solely for the information and use of management of Liquid Web and its clients and is not intended to be and should not be used by anyone other than these specified parties.

UHY LLP

Farmington Hills, Michigan
July 2, 2018

II. MANAGEMENT'S ASSERTION

Liquid Web's Assertion:

Liquid Web confirms that to the best of our knowledge and belief, Liquid Web has implemented controls to address the General Data Protection Regulation ("GDPR") of the European Union ("EU"). The criteria we used in making this assertion were that

1) The risks that threaten the achievement of the controls related to GDPR have been identified by Liquid Web.

2) The controls related to the GDPR criteria would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated from being achieved.

III. EXAMINATION APPROACH, KEY FINGDINGS, SUMMARY OF RESULTS

Examination 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 and 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).

Our tests of the control environment included the following procedures, to the extent we considered necessary: (a) a review of Liquid Web'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 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 as of May 15, 2018.

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 GDRP 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 data outside of the United States as part of their standard services. All customer data for US customers stays within the United States, 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.

Summary of Test Results

Liquid Web was determined to have designed and implemented controls in place regarding their co-Location, web hosting, and network infrastructure services to address the General Data Protection Regulation ("GDPR") of the European Union ("EU") as of May 15, 2018.

The table below outlines the applicable GDPR Article, key points for each article and the Liquid Web controls implemented to address the GDPR requirements.

Key Processor Requirements and Controls
Article 28 - Processor
The processor shall not engage another processor without prior specific or general written authorization of the controller.
Each Liquid Web 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 Liquid Web website for external users.
Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.
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.
Each Liquid Web 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 Liquid Web website for external users.
Security and availability commitments made to external users are communicated within the Terms of Service, which is provided to external users upon onboarding.
Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.
The processor adheres to an approved code of conduct.
New hires sign an acknowledgement upon hire to acknowledge they will abide by the information security policies and conduct standards.
Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.
Article 29 - Processing under the authority of the controller or processor
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.
Each Liquid Web 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 Liquid Web website for external users.
Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.
Article 31 - Cooperation with the supervisory authority
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.
Liquid Web maintains procedures for reporting operational failures, incidents, and system problems.
A formal Incident Response Plan was in place. The Incident Response Plan documents the procedures for issue identification and resolution. Additionally, the plan includes procedures for notifying the appropriate personnel and customers.
Article 32 - Security of processing
Personal data is secured through the use of pseudonymisation and encryption.
All authorized users of Liquid Web Network are identified and authenticated via a unique user ID and password. Access to hosting related systems and infrastructure is further restricted via two factor authentication using IDM. IDM User IDs are unique and passwords are encrypted.
An encryption key is utilized for authenticating to Liquid Web's network. Each encryption key for RADIUS authentication servers are generated randomly via an automated script to encrypt passwords.
Remote access is controlled via VPN software which requires two factor authentication. VPN for remote access utilizes AES encryption.
The processor ensures the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
Quarterly external network assessments are conducted. Additionally, internal vulnerability scanning is performed continuously for assets and networks. Remediation efforts of issues found are documented by IT management.
Weekly department head meetings are conducted to discuss current issues and assign responsibilities for resolving them, including development and modification of security and availability policies and performance issues that are unresolved.

Key Processor Requirements and Controls
Executive Management is responsible for monitoring trends in the hosting services industry and identifying risks internally and externally.
The Security Team is following the NIST Feed, US Cert Feed, and facilities would track the weather with an on call rotation if there is severe weather. An email notification would be sent out if there is something that needs to be documented as far as regulatory or environmental trends.
Liquid Web uses an issue tracking system to record and monitor security and availability issues through resolution. Any unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.
Weather monitors are mounted on the walls throughout the facility to monitor for severe weather. Additionally, the Facilities Team monitors the weather for natural disaster preparedness.
Server failure monitoring, disk space monitoring, load monitoring, and memory available monitoring is performed by the Sonar Monitoring™ Team. Alerts are tracked to resolution within the ticketing system.
Network uptime is monitored in real- time by the Networking team.
Future capacity needs are tracked by IT management as a part of inventory management.
Network authentication is controlled via redundant RADIUS servers controlled exclusively by the network engineering and system operations groups.
An encryption key is utilized for authenticating to Liquid Web's network. Each encryption key for RADIUS authentication servers are generated randomly via an automated script to encrypt passwords.
Firewalls are in place to protect the internal Liquid Web network. Administrator access to the firewalls is restricted to the Network Engineering Team.
Firewall and network device configuration log files are monitored and reviewed by the Networking Managers on a daily basis. The review is documented within the End of Shift Reports.
An Intrusion Prevention System (IPS) is in place and sends alerts to Security personnel for high and critical severity vulnerabilities. Administrator access to the IPS was restricted to authorized Security personnel.
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.
A weekly review of Liquid Web internal system and infrastructure configuration backup jobs is performed by management to ensure that all scheduled internal systems and infrastructure backups were successfully performed.
Backup data for Liquid Web internal systems and infrastructure are maintained at an alternate Liquid Web datacenter. Access to backup data is restricted to authorized employees.
Annually, Liquid Web performs a tabletop test of system redundancy to ensure the system remains available to customers.
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.
A weekly review of Liquid Web internal system and infrastructure configuration backup jobs is performed by management to ensure that all scheduled internal systems and infrastructure backups were successfully performed.
Backup data for Liquid Web internal systems and infrastructure are maintained at an alternate Liquid Web datacenter. Access to backup data is restricted to authorized employees.
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 conducted. Additionally, internal vulnerability scanning is performed continuously for assets and networks. Remediation efforts of issues found are documented by IT management.
Weekly department head meetings are conducted to discuss current issues and assign responsibilities for resolving them, including development and modification of security and availability policies and performance issues that are unresolved.
Server failure monitoring, disk space monitoring, load monitoring, and memory available monitoring is performed by the Sonar Monitoring™ Team. Alerts are tracked to resolution within the ticketing system.
Network uptime is monitored in real- time by the Networking team.
An Intrusion Prevention System (IPS) is in place and sends alerts to Security personnel for high and critical severity vulnerabilities. Administrator access to the IPS was restricted to authorized Security personnel.

Key Processor Requirements and Controls
A weekly review of Liquid Web internal system and infrastructure configuration backup jobs is performed by management to ensure that all scheduled internal systems and infrastructure backups were successfully performed.
Annually, Liquid Web performs a tabletop test of system redundancy to ensure the system remains available to customers.
Employees are required to attend security awareness training upon hire and on an annual basis.
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.
New users and employees are requested by Human Resources/employee's manager through the Office IT department. The Office IT department assigns users to a LDAP group profile based on their department.
All authorized users of Liquid Web Network are identified and authenticated via a unique user ID and password. Access to hosting related systems and infrastructure is further restricted via two factor authentication using IDM. IDM User IDs are unique and passwords are encrypted.
Access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.
Administrator access to the Liquid Web Network and authentication systems is restricted to authorized users.
User access reviews are performed annually by the Department Heads to determine if access privileges are appropriate. Any modifications in access are performed by the Office IT department.
Physical access to the building and data center is monitored by an on premise security guard and and/or Infrastructure team personnel via the recorded video surveillance system.
Visitors are required to show a valid ID and are provided with a photo ID with a visitor badge upon entry to the Liquid Web facility. Visitors are escorted for the duration of their visit. Additionally, visitor profiles are visible via the building monitor so employees are aware of the visitors currently in the building.
Access to the data center is restricted to technical staff.
The processor adheres to an approved code of conduct.
New hires sign an acknowledgement upon hire to acknowledge they will abide by the information security policies and conduct standards.
Liquid Web's conduct standards are reviewed annually, updated as necessary, and approved by management. Employees are required to acknowledge and agree to the conduct upon hire and major change.
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.
Each Liquid Web 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 Liquid Web website for external users.
Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.
Article 33 - Notification of a personal data breach to the supervisory authority
The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
Changes to security and availability requirements or commitments are communicated to internal and external users via email.
Data Processing Agreements outlining the controller and processor responsibilities have been developed and are entered into by Liquid Web upon request from the controller.
Liquid Web maintains procedures for reporting operational failures, incidents, and system problems.
A formal Incident Response Plan was in place. The Incident Response Plan documents the procedures for issue identification and resolution. Additionally, the plan includes procedures for notifying the appropriate personnel and customers.
Article 35 - Data protection impact assessment
Data protection impact assessment are conducted periodically.
A risk assessment is performed on an annual basis which includes evaluating the threats applicable to major infrastructure assets, the network, and user workstations for the impact, severity, and likelihood. The Infrastructure and Security Teams are responsible for identifying risks and controls to mitigate those risks identified.
Annually, Liquid Web performs a tabletop test of system redundancy to ensure the system remains available to customers.
Compliance with approved codes of conduct are taken into due account in assessing the impact of the processing operations.
New hires sign an acknowledgement upon hire to acknowledge they will abide by the information security policies and conduct standards.

Key Processor Requirements and Controls
Liquid Web's conduct standards are reviewed annually, updated as necessary, and approved by management. Employees are required to acknowledge and agree to the conduct upon hire and major change.
Article 37 - Designation of the data protection officer
The processor shall designate a data protection officer(s).
Liquid Web has implemented a data protection and privacy team. The team meets regularly and are responsible for handling issues related to data protection and privacy.
Article 40 - Codes of conduct
An approved code of conduct is in place an acknowledged by the processor's employees.
New hires sign an acknowledgement upon hire to acknowledge they will abide by the information security policies and conduct standards.
Liquid Web's conduct standards are reviewed annually, updated as necessary, and approved by management. Employees are required to acknowledge and agree to the conduct upon hire and major change.
Article 41 - Monitoring of approved codes of conduct
The code of conduct is reviewed periodically, updated as necessary, and approved by management.
New hires sign an acknowledgement upon hire to acknowledge they will abide by the information security policies and conduct standards.
Liquid Web's conduct standards are reviewed annually, updated as necessary, and approved by management. Employees are required to acknowledge and agree to the conduct upon hire and major change.
A performance review is performed and documented by each department head on an annual basis.