Copyleaks LTD.

Copyleaks platform

ISAE 3000 (SOC 3)

Service Auditor's Assurance Report

For the period

October 1, 2023, to December 31, 2023

Contents

SOMEKH CHAIKIN
KPMG Millennium Tower
17 Ha'arba'a Street
Tel Aviv, 6473917, Israel

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Section I – Independent Service Auditor's Report

To the Management and board of directors of Copyleaks LTD.:

We have examined management's assertion that Copyleaks LTD., during the period October 1, 2023, to December 31, 2023, maintained effective controls to provide reasonable assurance that:

- The System was protected against unauthorized access, use, or modification.
- The System was available for operation and use, as committed or agreed.
- Information within the System designated as confidential is protected as committed or agreed.

Based on the criteria for Security, Availability, Confidentiality and Privacy n the American Institute of Certified Public Accountants' TSP Section 100 (2017), Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Copyleaks LTD.management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) Obtaining an understanding of Copyleaks LTD. relevant to security, availability, confidentiality, and Privacy controls.

(2) Testing and evaluating the operating effectiveness of the controls.

(3) Performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Copyleaks LTD. management's assertion referred to above is fairly stated, in all material respects, based on the mentioned criteria for security, availability and confidentiality.

Yours faithfully,

KPMG

Tel Aviv, Israel

February 5, 2024

Section II - Management Assertion Provided by Copyleaks LTD.

We, as management of, Copyleaks LTD. ("the Company") are responsible for:

- Identifying the Copyleaks LTD. SaaS Platform (“the system”) and describing the boundaries of the system.
- Identifying our principal service commitments and system requirements.
- Identifying the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of our system.
- Identifying, designing, implementing, operating, and monitoring effective controls over the Copyleaks LTD. platform (system), to mitigate risks that threaten the achievement of the principal service commitments and system requirements.
- Selecting the trust services categories that are the basis of our assertion.

We assert that the controls over the system were effective throughout the period October 1, 2023, to December 31, 2023, to provide reasonable assurance that the principal service commitments and system requirements were achieved, based on the criteria relevant to Security, Availability, Confidentiality and Privacy set forth in the AICPA’s TSP Section 100 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016).

Copyleaks LTD.

February 5, 2024

Section III - Description of Copyleaks LTD. system

Company Overview and Background

Copyleaks is an AI based content authentication platform that is focused on detection of originality in textual content.

Key Features of Copyleaks platform

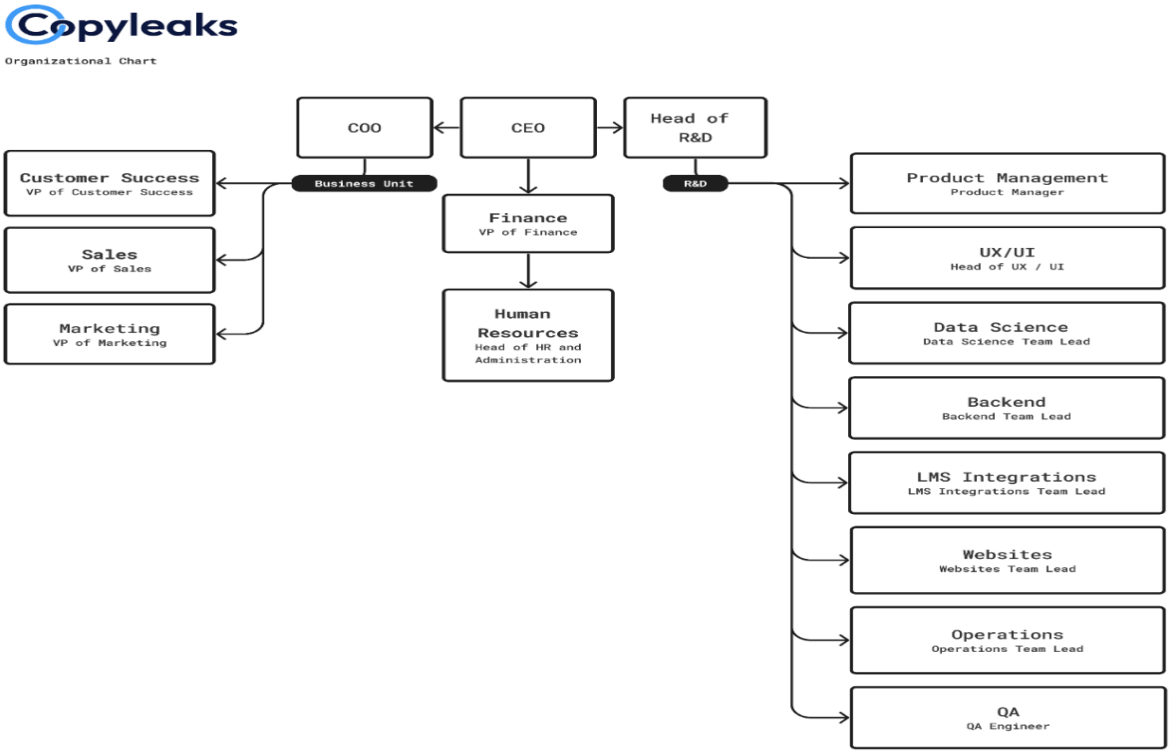
Copyleaks serves as an advanced text analysis platform with a diverse range of use cases. Copyleaks key features include:

1. Plagiarism Detection- refers to the process of identifying and determining instances of plagiarism in written or creative works.
2. AI Content Detection
3. Grammar Correction
4. LMS (Learning Management System) Integrations
5. API
6. Teams
7. Repositories
8. Gen-AI Governance

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting Copyleaks platform and does not extend to other products and services or the controls at third-party service providers.

Organizational Structure



Copyleaks organizational structure provides the overall framework for planning, directing, and controlling operations. It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers. It represents the system through which employees, management, and operations interact to achieve business objectives. The structure clearly defines the lines of authority, responsibility, and communication, and provides the overall framework for planning, directing and controlling operations. Operating under this strategic design enables Copyleaks to utilize its time and resources effectively to support its customers and progressively enhance the solutions offered to them. An organization chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.

Sales: The sales department is composed of specialized and experienced sales personnel. It is responsible for selling and optimizing sales to Copyleaks' potential customers.

Marketing: The marketing department is responsible for building the company's brand, generating sales leads, and other marketing activities.

Customer Success/Support: The CS team is responsible for providing support to Copyleaks customers. The support team is working closely with R&D and QA.

Product: The product team is responsible for defining the Copyleaks product lines and available services - requirements and priorities.

Research and Development (R&D): The R&D department is responsible for developing Copyleaks products and the business services implemented within the production environment. This department includes two development teams as detailed below:

- Server side: This team is in charge of the development that concerns the server side, providing all the facilities and security features needed for the product delivery.
- Client side: This team is in charge of the web page and functions performed on the client's side as well on the desktop client application.
- Quality Assurance (QA): The QA department is responsible for testing and validating the R&D's deliverables according to predefined scenarios. The QA personnel are an integral part of R&D teams and are mentored by the CTO overseeing the entire QA activities at Copyleaks.

Finance & Admin Team: The Finance and Admin department is responsible for the company's legal, compliance, financial and control activities including financial planning and administrative tasks.

Description of the Control Environment, Information Communication, Monitoring and Risk Assessment Process

Copyleaks' internal control is a process affected by the entity's boards of directors, management, and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable Google Cloud Platform and regulations. The following section is a description of the five components of internal control for Copyleaks.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning the importance of controls and the emphasis given to controls in the entity's policies, procedures,

methods, and organizational structure. Copyleaks executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Policies and procedures documents for significant processes that address system requirements and relevant updates are available on the internal intranet. Policies and procedures are documented, reviewed, approved on an annual basis by the management team, and available to Copyleaks employees within the Copyleaks shared Google drive.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through Copyleaks:
(1) Management operating style;
(2) Organizational structure;
(3) Employee job descriptions and;
(4) Organizational policies and procedures.

Board of Directors: The Board of Directors (BOD) of Copyleaks is composed of both external directors and directors who are executive officers of the Company. The external directors are both: (1) Industry experts; (2) Investor representatives. The Board of Directors is actively engaged in the governance of the Company and its strategic direction. The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations. It has sufficient members who are independent from management and objective in evaluations and decision making. Members of the Board meet on at least a quarterly basis to discuss matters pertinent to the Company and to review financial information. Part of the Board's mission is to define, maintain and periodically evaluate the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action. The Board's responsibilities include but are not limited to (1) monitoring the actual performance of the Company through its financial results; (2) monitoring the Company's compliance with legal and regulatory requirements; (3) analysis of the budget vs actual results; (4) guiding the Company in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with the Company, including, without limitation, employment agreements, severance agreements, change in control agreements and restrictive covenants and (6) approving equity-based compensation plans in which directors, officers or employees may participate. The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control. The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the standards of conduct. Company board of directors meets on a semi-annual basis. The board meeting has a fixed agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) the product discussion with new features (**1**).

Management Philosophy and Operating Style: The Management Team, chaired by the Chief Executive Officer ("CEO"), has been delegated by the Board the responsibility to manage Copyleaks and its business on a daily basis. Copyleaks is led by a team with proven ability in media and online customer solutions to the global market. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand Copyleaks objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. The Management Team convenes on a weekly basis or more frequently if necessary.

Integrity and Ethical values: Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of Copyleaks ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities. These include management's actions to remove or reduce inappropriate incentives or extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the organization's values and

behavioral standards to personnel through policy statements and from the executives. The Board of Directors and Management Team recognize their responsibility to foster a strong ethical environment within Copyleaks to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct.

Human Resources Policy and Practices: Human resource policies and practices relate to hiring, orienting, training, evaluating, promoting, and compensating personnel. The competence and integrity of Copyleaks personnel are essential elements of its control environment. The organization's ability to recruit and retain highly trained, competent, and responsible personnel is dependent to a great extent on its human resource policies and practices. Teams are expected to adhere to the Copyleaks policies that define how services should be delivered and products need to be developed. These are located on the Copyleaks platform and can be accessed by relevant Copyleaks team members while communicated by emails or other messaging applications, such as Slack, on an as-needed basis. Internal employees sign on an NDA as part of their employment contract with the Company while clients and 3rd parties sign on NDA within the business contract.

Commitment to Competence: Competence at Copyleaks is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. Job descriptions are documented and maintained. Candidates go through screening and appropriate background checks based on regulations in the Country the company hires personnel.

Risk Assessment

Risk assessment: The process of identifying, assessing, and managing risks is a critical component of Copyleaks internal control system. The purpose of Copyleaks risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of Copyleaks and include regular management and supervisory activities. Managers of each department are regularly in touch with personnel and may question the accuracy of information that differs significantly from their knowledge of operations. Minutes of risk assessment meetings and action items are documented into emails. On an annual basis risks are reviewed and updated in order to, among others, re-assess risks, review operational aspects of the control environment, and monitor the control environment.

Risk Mitigation

Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity or the likelihood of the risk occurring, and the control activities necessary to mitigate the risk are identified. Copyleaks selects and develops control activities that contribute to the mitigation of risks to the achievement of the company's objectives to acceptable levels. The risk mitigation process is integrated with the company's risk assessment. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Copyleaks' objectives during response, mitigation, and recovery efforts. Copyleaks requires Third party Vendors to have a valid SOC2 certification.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks to the achievement of the entity's objectives.
Copyleaks operating and functional units are required to implement control activities that help achieve business objectives associated with:
(1) The reliability of financial reporting,

(2) The effectiveness and efficiency of operations and
(3) Compliance with applicable Google Cloud Platform and regulations.

The controls activities are designed to address specific risks associated with Copyleaks operations and are reviewed as part of the risk assessment process. Copyleaks has developed formal policies and procedures covering various operational matters to document the requirements for performance of many control activities. New employees go through a boarding process during which, among others, are communicated their responsibilities and the different Copyleaks policies.

Information and Communication

Information and communication are an integral component of Copyleaks internal control system. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage and control the organization's operations. At Copyleaks, information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, vendors, regulators and employees. The management team meets on at least a monthly basis, in order to evaluate risks and threats and discuss security and non-compliance issues and address them. Minutes of the meeting are retained.
Senior executives who lead the meetings use information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to organization-wide security policies and procedures are usually communicated to the appropriate Copyleaks personnel via dedicated system.

Monitoring

Copyleaks uses a monitoring tool to monitor Copyleaks Platform. Alerts are sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. The notifications are reviewed and addressed according to their level of urgency. Metrics produced from these systems are used to identify the strengths and achievements as well as the weaknesses, inefficiencies, or potential performance issues with respect to a particular process. Managers are given the responsibility to inform the individuals who report to them about these items at the appropriate time. The Copyleaks Management Team monitors the progress with respect to Copyleaks Service processes on a regular basis. Analysis of root cause is performed through various tools and meetings, and corrective measures are communicated to relevant groups through emails, meetings, and a project portal tool in order to prevent future occurrences. Changes impacting customers are communicated to clients through release notes within the Copyleaks Platform or by email. While internal employees receive notifications through a dedicated system.

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Assets are assigned owners to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee devices that may contain personal data. When assets reach end of life, they are securely destroyed to ensure that data is not recoverable.

Antivirus

EDR is implemented on employees laptops to prevent or detect and act upon the introduction of unauthorized or malicious software.

Support

Copyleaks customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, or issues submitted by clients. Client issues are documented within the CRM tool. Cases are prioritized and processed based on the internal support policy.

Ticketing and Management

Copyleaks opens a ticket when an issue is raised by a client or when an issue is proactively identified. Copyleaks uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution. In addition, client's issues are documented. Cases are prioritized and processed based on the internal support policy.

Database Backup and restoration

Meta data retained in the database is dumped daily and stored into a bucket enabling geo redundancy. The backup system automatically generates a backup log. In case of failure, a notification is sent to the R&D team. Restore tests are performed on an annual basis. The test includes a full restore to a separate database server and bringing up the database to verify data integrity and accessibility as well as backup restoration test. Copyleaks perform backup in order to maintain full redundancy in different locations.

Data Protection Procedures

Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information. Transmission of data is a key aspect of Copyleaks' internal controls. Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points. The transmission of data can be performed through removable media as well as through mobile devices. Processes are in place to protect mobile devices (such as laptops, smartphones, and tablets) that serve as information assets. When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.

Disaster Recovery Plan (DRP)

Copyleaks has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis. Copyleaks maintains a backup at a separated location within the Google Cloud Platform environments. The backup file has been designed to allow full functionality of the Copyleaks platform in case of a disaster in the main data center. Copyleaks documents and approves on an annual basis a restore document describing the required steps in order to perform a restore.

Privacy

Organization has appointed a Privacy Officer who is accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disclosure of personal information.

Copyleaks collects personal information in accordance with the organization's privacy commitments. Consents obtained from data subjects for collection, usage and disclosure of personal information are retained in accordance with privacy laws and regulations as well as objectives defined in the privacy policy.

Copyleaks describes the purposes for which personal information is collected, used, maintained, and disclosed in its Privacy Policy.

Copyleaks has documented and implemented a privacy risk assessment process to assess risks resulting from the collection, storage, transmission, use and disclosure of personal information. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.

Sub-service organizations carved-out control:

Google Cloud Platform

Copyleaks hosts the application data primarily in Google Cloud Platform data centers which are certified as ISO 27001, PCI DSS Service Provider Level 1, and is SOC 2 compliant.

Business continuity plan arrangements in Google Cloud Platform have been reviewed and approved by Copyleaks and Google Cloud Platform specialists and are implemented in all Copyleaks backups processes.

#	Control Activity Expected to be Implemented by Google Cloud Platform (Subservice organization)	Applicable Trust Service Criteria
1	Subservice organizations are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its infrastructure as a Service (IaaS) cloud hosting services where Information systems reside.	CC6.1 – CC6.4, CC6.6
2	Subservice organizations are responsible for implementing and maintaining environmental protection.	A1.3
3	Subservice organizations are responsible to revoke access to the scoped data centers in a timely manner of employee or vendor record being deactivated.	CC6.2
4	Subservice organizations are responsible to periodically review access to the scoped data center by appropriate personnel.	CC6.2
5	Subservice organizations are responsible for monitoring and maintaining processing capacity on an ongoing basis.	A1.1
6	Subservice organizations are responsible for notify of unauthorized use of any account or other breaches related to the security, availability, confidentiality, and Privacy in service usage.	CC7.1 - CC7.5
7	Subservice organizations are responsible for installing anti-malware solutions to detect or prevent unauthorized or malicious software on hosted systems	CC6.8
8	Subservice organizations are responsible for implementing strong authentication mechanisms.	CC6.1
9	Subservice organizations are responsible for monitoring backup operations and alerting of backup failures	A1.3

User Entity Responsibilities

#	User Entity Responsibilities	Related Complemented Criteria Ref. Number
1	Ensure strong password policy.	CC6.1
2	Ensure multi-factor Authentication.	CC6.1
3	Ensure timely removal of user accounts for employees when user access is no longer required.	CC6.2
4	Configure roles and authorization – configure access to be based on the individual's roles and responsibilities and be limited to the minimum access right necessary to perform an assigned job function.	CC6.3
5	Secure on-premises components.	CC6.1, CC6.8, CC7.1
6	Integrating with monitored platforms/applications in a secure manner and according to necessary compliance requirements.	CC6.1, CC6.7
7	Notify Copyleaks of unauthorized use of any account or other breaches related to the security, availability, and confidentiality in service usage.	CC4.2, CC7.2, CC7.4