DATA PRIVACY AGREEMENT
BETWEEN THE IRVINE UNIFIED SCHOOL DISTRICT

AND

CHECK POINT SOFTWARE TECHNOLOGIES, INC.

WHEREAS, the Irvine Unified School District ("District") and Check Point Software Technologies, Inc. ("Provider") have entered into an agreement ("Agreement") dated August 30, 2022 wherein Provider will perform cloud security services (the "Service(s)"); and

WHEREAS, in order to provide the Service described above, Provider may have access to student information, such information generally limited to the data elements listed in Section 13 of this Data Privacy Agreement ("Student Data"), defined as student records under the Family Educational Rights and Privacy Act (FERPA) and California Education Code § 49073.1, among other statutes, which are therefore subject to statutory protection; and

WHEREAS, the parties wish to execute this Data Privacy Agreement ("DPA"), effective as of August 30, 2022, in full compliance with FERPA, California Education Code § 49073.1, and other applicable data privacy laws.

NOW THEREFORE, for good and valuable consideration, the Parties agrees as follows:

PURPOSE

1. District and Provider agree to uphold their responsibilities under all applicable privacy statutes, including FERPA, the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and AB 1584 (found in Education Code Section 49073.1).

DATA PRIVACY

2. Data Property of District: All Student Data, information, data, and other content provided or transmitted by the District to the Provider, or entered or uploaded under District's user accounts ("Data"), remain the sole property of the District. The District retains exclusive control over Student Data and Data including personal information of District staff, including determining who may access Student Data and how it may be used for legitimate authorized purposes. A parent, legal guardian or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and request the transfer of pupil-generated content to a personal account.

3. Data Access: Provider may access District Data solely to fulfill its obligations under the Agreement.

4. Third Party Access: Provider may not distribute District Data or content to any third party without District's express written consent, unless required by law, and except to subcontractors who have agreed to privacy terms consistent with those in this DPA. Provider will ensure that approved subcontractors adhere to all provisions of this DPA. Deidentified and aggregate information may be used by Provider for the purposes of development and improvement of educational sites, services or applications.

5. Third Party Request: Should a third party contact Provider with a request for District Data, including law enforcement and government entities, Provider shall redirect the third party to request the Data directly from the District unless legally prohibited. Provider shall notify the District in advance of a compelled disclosure to a third party unless legally prohibited.

6. Applicability of COPPA: Provider warrants to District that all data collected directly from children and/or data resulting from tracking children's use of the Service is subject to parental consent and will occur in strict conformity to the requirements of the Children's Online Privacy Protection Act (COPPA). Provider shall obtain such parental consent, unless expressly agreed to otherwise by the parties. Provider may not sell or market Student Data, or use Student Data for sale or marketing purposes, including but not limited to targeted advertising, without express parental consent. However, Provider is not restricted from using anonymous, disaggregate data for marketing purposes, provided that such data cannot be used to identify an individual student.

7. Authorized Use: Provider warrants that the data shared under the Agreement and this DPA shall be used for no purpose other than providing the Service pursuant to the Agreement and/ or otherwise authorized under the statutes referred to in section 1, above.

8. Employees Bound: Provider shall require all employees of Provider and subcontractors who may have access to Student Data to comply with all applicable data privacy laws with respect to the data shared under this DPA.

9. Secure Environment: Provider shall maintain all Data obtained pursuant to this DPA in a secure computer environment and not copy, reproduce or transmit Data obtained pursuant to this DPA except as necessary to provide the Service pursuant to the Agreement. Provider has security measures in place to help protect against loss, misuse and alteration of the Data under Provider's control. When the Service is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology protects information, using both server authentication and data encryption to help ensure that Data is safe, secure, and available to only authorized users. Provider shall host the Service in a secure server environment that uses a firewall and other advance technology in an effort to prevent interference or access from outside intruders. The Service will require unique account identifiers, usernames and passwords that must be entered each time a client or user signs on.

10. Disposition of Data: Provider shall destroy all Student Data and/or personally identifiable Data obtained under the Agreement and/or this DPA when it is no longer needed to perform the Services, and no later than 60 days following the expiration or termination of the Services provided under the Agreement, unless a reasonable written request for destruction or retention of data is submitted by the District. Nothing in the Agreement or this DPA authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

11. Data Breach Notification: Upon becoming aware of any unlawful or unauthorized access to District Data in possession of Provider and/or stored on equipment used by Provider or in facilities used by Provider, Provider will: notify the District as promptly as possible of the suspected or actual incident; investigate the incident as promptly as possible and provide District with detailed information regarding the incident, including the identity of affected users; provide assistance to the District in notifying affected users by taking commercially reasonable steps to mitigate the effects and to minimize any damage resulting from the incident in accordance with Provider's Data Security Policy. Provider shall obtain permission from District prior to directly notifying users of a breach, unless such notice is required by law.

12. Audit: The District reserves the right to audit and inspect the Provider's compliance with this DPA and applicable laws upon reasonable prior written notice to Provider's principal place of business, during normal business hours, and no more than once per year.

13. Data Requested: Names, usernames and IP Addresses of the District's employees and students using the cloud service; email sender, recipient and body of email if so configured and any attachments or URLs in the body of an email the system inspects.

DISTRICT DUTIES

14. District: The District will perform the following duties:

(a) Provide Data: Provide data for the purposes of utilizing the Service in compliance with FERPA.

(b) Precautions: Take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Service and hosted data.

(c) Notification: Notify Provider as promptly as possible of any known or suspected unauthorized access.

AGREEMENT

15. Term The Provider shall be bound by this DPA for the duration of the Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than five (5) years.

16. Priority of Agreements: The Agreement and this DPA shall govern the treatment of Student Data in order to comply with the applicable privacy protections, including those found in FERPA and California Education Code § 49073.1. In the event there is conflict between the terms of this DPA and the Agreement or any other Bid/RFP, license agreement, or contract document(s) in existence, the terms of this DPA shall apply solely with respect to the personally identifiable data provided under the terms of the Agreement.

17. Successors Bound: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

18. Modification of Agreement: No modification or waiver of any term of this DPA is effective unless mutually agreed to in writing by both parties.

19. Severability. If any term, condition or provision of this DPA is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions will nevertheless continue in full force and effect, and shall not be affected, impaired or invalidated in any way.

20. Governing Law. The terms and conditions of this DPA shall be governed by the laws of the State of California with venue in Orange County, California. This DPA is made in and shall be performed in Orange County, California.

21. Non Waiver. The failure of District or Provider to seek redress for violation of, or to insist upon, the

strict performance of any term or condition of this DPA, shall not be deemed a waiver by that party of such term or condition, or prevent a subsequent similar act from again constituting a violation of such term or condition.

IN WITNESS WHEREOF, the parties have executed this Data Privacy Agreement as of August 30, 2022.

IRVINE UNIFIED SCHOOL DISTRICT

By: ______________________ Date: June 28, 2022

Printed Name: John Fogarty Title/Position: Asst. Supt. Business Services

IUSD Board Approved July 12, 2022

CHECK POINT SOFTWARE TECHNOLOGIES, INC.

By: ______________________ Date: 06/22/2022

Printed Name: Philip Levine Title/Position: Head of Finance, Americas

Note: Electronic signature not permitted.

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR (g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2021

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from ________ to ________

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Date of event requiring this shell company report ________
Commission file number 000-28584

CHECK POINT SOFTWARE TECHNOLOGIES LTD.
(Exact name of Registrant as specified in its charter)

ISRAEL
(Jurisdiction of incorporation or organization)

5 Shlomo Kaplan Street Tel Aviv 6789159, Israel
(Address of principal executive offices)

Shira Yashar, Adv.
General Counsel
Check Point Software Technologies Ltd.
5 Shlomo Kaplan Street Tel Aviv 6789159, Israel
Tel: (+972) 3-753-4555 (Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered or to be registered pursuant to Section 12(b) of the Act.

Title of each class	Trading symbol(s)	Name of each exchange on which registered
Ordinary shares, NIS 0.01 nominal value	**CHKP**	**NASDAQ Global Select Market**

Securities registered or to be registered pursuant to Section 12(g) of the Act. None

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act. None

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of December 31, 2021. 129,065,690 ordinary shares, nominal value NIS 0.01 per share.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act: Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934: Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No □

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No □

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or an emerging growth company. See definition of "large accelerated filer," "accelerated filer," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large Accelerated filer ☒ Accelerated filer □ Non-accelerated filer □ Emerging growth company □

If an emerging growth company that prepares its financial statements in accordance with U.S. GAAP, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards † provided pursuant to Section 13(a) of the Exchange Act. □

The term "new or revised financial accounting standard" refers to any update issued by the Financial Accounting Standards Board to its Accounting Standards Codification after April 5, 2012.

Indicate by check mark whether the registrant has filed a report on and attestation to its management's assessment of the effectiveness of its internal control over financial reporting under Section 404(b) of the Sarbanes-Oxley Act (15 U.S.C. 7262(b)) by the registered public accounting firm that prepared or issued its audit report. ☒

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing:

U.S. GAAP ☒ International Financial Reporting Standards as issued by the International Accounting Standards Board □ Other □

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 □ Item 18 □

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act): Yes □ No ☒

Auditor Firm Id: 1281 **Auditor Name:** Kost Forer Gabbay & Kasierer, a member of Ernst & Young Global

Check Point Press Releases

Avanan, Acquired by Check Point Software Technologies, Recognized as one of the Fastest-Growing Email Security Companies in North America on the 2021 Deloitte Technology Fast 500™

For the second consecutive year, Avanan's email security solution ranked in the top 500 fastest-growing technology companies in North America

SAN CARLOS, CA — Thu, 18 Nov 2021

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), a leading provider of cyber security solutions globally, today announced Avanan, recently acquired by Check Point Software, ranked 125 on the Deloitte Technology Fast 500™, a ranking of the 500 fastest-growing technology, media, telecommunications, life sciences, fintech, and energy tech companies in North America, now in its 27th year.

"Email has consistently been the number one attack vector leading to breaches in organizations, and Avanan's focus on securing cloud-based email has allowed us to lead the revolution in how organizations secure their email," said Gil Friedrich, VP of Email Security at Check Point Software Technologies. "Check Point Software and Avanan's industry-leading API-based security redefines cloud email security and delivers best-of-breed email malware protection. Organizations around the world can now modernize their legacy solutions with email security as-a-service and protect cloud email and collaboration suites from the most sophisticated attacks."

"Each year the Technology Fast 500 shines a light on leading innovators in technology and this year is no exception," said Paul Silverglate, vice chair, Deloitte LLP and U.S. technology sector leader. "In the face of innumerable challenges resulting from the pandemic, the best and brightest were able to pivot, reinvent and transform and grow. We celebrate the winning organizations and especially the talented employees driving their success."

“The pandemic has underscored the urgent need for tech solutions in a variety of areas across health care, fintech, energy tech, entertainment, to name a few, so reliance on innovators like the winners of the Technology Fast 500 is more important than ever,” said Christie Simons, partner, Deloitte & Touche LLP and industry leader for technology, media and telecommunications within Deloitte’s audit & assurance practice. “These companies are not only at the cutting edge, transforming the way we do business, but most importantly, recognize the strategic importance of ongoing innovation, especially in the ever-changing world of technology.”

Avanan previously ranked 171st as a Technology Fast 500™ award winner for 2020.

Overall, 2021 Technology Fast 500™ companies achieved revenue growth ranging from 212% to 87,037% from 2017 to 2020, with median growth of 521%.

Now in its 27th year, the Deloitte Technology Fast 500 provides a ranking of the fastest-growing technology, media, telecommunications, life sciences, fintech, and energy tech companies — both public and private — in North America. Technology Fast 500 award winners are selected based on percentage fiscal year revenue growth from 2017 to 2020.

In order to be eligible for Technology Fast 500 recognition, companies must own proprietary intellectual property or technology that is sold to customers in products that contribute to a majority of the company’s operating revenues. Companies must have base-year operating revenues of at least US$50,000, and current-year operating revenues of at least US$5 million. Additionally, companies must be in business for a minimum of four years and be headquartered within North America.
&

Follow Check Point via:

Twitter: https://www.twitter.com/checkpointsw

Facebook: https://www.facebook.com/checkpointsoftware

Blog: https://blog.checkpoint.com

YouTube: https://www.youtube.com/user/CPGlobal

LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers multilevel security architecture, "Infinity" Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.