**Kaspersky Labs Limited**

**Strategic Report and Corporate Governance Report**

**FINANCIAL YEAR 2021**

Kaspersky Labs Limited (the “Company”), a private company limited by shares, and its subsidiaries all over the world (together referred to as the “Group” or “Kaspersky”) comprise of private limited companies in accordance with The Companies Act 2006 located in the UK.

The Company’s registered office is: 2 Kingdom Street, London, W2 6BD.

Kaspersky is one of the world’s largest privately-owned cybersecurity companies, with the company registered in the United Kingdom.

The Group was founded in 1997 and today it is an international group operating in almost 200 countries and territories worldwide. It has 34 representative territory offices in more than 30 countries. Kaspersky has a corporate client base of more than 240,000 companies located around the globe, ranging from small and medium-sized businesses to large governmental and commercial organizations. Over 400 million people worldwide are protected by Kaspersky products and technologies. Kaspersky currently employs more than 4,000 qualified specialists. More than a third of the highly qualified specialists working at Kaspersky are research and development (R&D) specialists developing and maintaining all of our solutions in-house, which is key to providing a holistic approach to security.

The Group’s portfolio encompasses solutions to suit a wide range of customers, protecting consumers, small companies, medium-sized businesses and enterprises from different types of threats and provides them with convenient tools to control and manage their security.

Kaspersky empowers consumers with a range of products to protect all corners of their lives from cybercrime. It understands the needs of small businesses and has a unique multi-layered solution especially for them, which unites ease of management and effective protection. The Group covers all the cybersecurity needs of large enterprises with its full enterprise platform that helps to prevent all types of cyberthreats, detects even the most sophisticated attacks, responds to security incidents and predicts the evolution of the threat landscape. The Group’s comprehensive portfolio of solutions achieves all of this thanks to the combination of our expertise, threat intelligence and machine learning that enables us to develop robust technologies to detect, block and prevent cyberattacks. The business focus of Kaspersky is continuing to evolve from “cybersecurity” towards the wider concept of “cyber-immunity”.

Almost half of the team working at Kaspersky are research and development (R&D) specialists developing and maintaining all of our solutions in-house, which is key to providing a holistic approach to security. An elite group of more than 40 security experts from our Global Research and Analysis Team (GReAT) operate all around the world and provide leading threat intelligence and research. The team is well-known for the discovery and dissection of some of the world’s most sophisticated threats, including cyber-espionage and cyber-sabotage threats.

To record the groundbreaking malicious cyber-campaigns that have been investigated by GReAT, Kaspersky launched a Targeted Cyberattack Logbook. Although our key expertise is related to cyberthreats, we fight against them not only to ensure that our customers are protected now, but so that our solutions are also ready for new challenges in the future. Today, it is more important for us to use this accumulated expertise to create technologies that will make cyberthreats lose their relevance.

Kaspersky is focused on innovation and believes in the collaboration with brilliant minds to accelerate the development of new solutions for a digitally safe today and tomorrow. Within Kaspersky Product Studio, a special unit aimed at exploring and creating new digital products for the company’s ecosystem, we discover new frontiers and identify new trends, understanding market needs, security challenges and demands across industries. We aim to develop solutions not only for the cybersecurity sector but also for IoT, fintech, legal tech, health tech, digital communications and smart homes.

Management believes that collaboration is the most effective way to fight cybercriminals. To this end, the Group shares its expertise, knowledge and technical findings with the world’s security community. Kaspersky was included in the list of Vulnerability Top Contributors by [Microsoft](https://msrc-blog.microsoft.com/2019/07/25/microsoft-announces-top-contributing-partners-in-the-microsoft-active-protections-program-mapp/).

Kaspersky cooperates with INTERPOL in the joint fight against cybercrime. The company provides the organization with human resources support, training, and threat intelligence data on the latest cybercriminal activities. Other partners in the field of law enforcement include, but are not limited to the Microsoft Digital Crimes Unit, as well as Computer Emergency Response Teams (CERTs) and many other police authorities worldwide.

By joining forces, the Group helped fighting cybercrime (such as the Carbanak case), disrupt criminal botnets (for example, Simda), and launch new initiatives (such as [No More Ransom](https://www.nomoreransom.org), with more than 100 supporting partners from the public and private sector). The Group takes part in joint cyberthreat investigations and conducts trainings for cybersecurity specialists. Collaboration between the Dutch police and Kaspersky led to the arrest of suspects behind the CoinVault ransomware attacks.

Kaspersky is involved in the discussion and development of cybersecurity initiatives and standards through its advisory group memberships (i.e. the Anti-Malware Testing Standards Organization). Aiming to solve the cyber security challenges faced by the modern world today, Kaspersky is also a member of initiatives and organizations such as Securing Smart Cities, the Industrial Internet Consortium and AUTOSAR.

The key markets where Kaspersky operates include:

* Сonsumer digital life protection (CDLP), previously categorized as consumer endpoint security, captures the broader set of technologies that vendors offer to consumers to address a range of consumers' cybersecurity and digital protection and privacy needs. Currently CDLP technologies include endpoint device security (i.e., antivirus), connected home security, parental controls, password management, cloud backup, identity protection, consumer VPN, and device care. CDLP vendors offer each technology as a separate product and/or tiered product packages of CDLP technologies and features.
* Endpoint Security products protect against both file-based and file-less malware. In the corporate segment, the endpoint security market is also increasingly associated with the Endpoint Detection & Response (EDR) market. EDR products facilitate incident investigation and remediation on endpoints in cases where threats successfully evade prevention controls.
* Managed Detection and Response (MDR) delivers advanced, round-the-clock protection from the growing volume of threats circumventing automated security barriers, providing detection and response capabilities and supported by hunting team.
* Web security – web security products are deployed on software, appliance, SaaS, and virtual platforms. Web security products may be capable of URL filtering, web anti-malware, web application firewall, and web content filtering. Select data loss prevention technologies can be included in web security as well. Web security products protect against both inbound (malware) and outbound (data leakage) threats.
* Messaging security – solutions are deployed on various types of messaging platforms. Product functionalities may include anti-spam, anti-malware, and content filtering. Messaging security products may also contain select data loss prevention, alongside select information protection and control technologies. These products are designed to work with applications, including email, instant messaging (IM), and other collaborative applications.
* Threat Intelligence Services – services for provisioning of information about potential cyber threats, including existing and emerging threats, cybercrime actors, tools and methods. This information can be used to inform decisions regarding the client’s response to those menaces / hazards. Threat intelligence is made available through portals, online delivered feeds, subscription-based analyst personnel support and platform software.
* Hybrid Cloud Security (Cloud Workload Protection) – Kaspersky Hybrid Cloud Security provides efficient virtual and cloud workload protection, visibility and control for hybrid IT infrastructures, with no adverse impact on systems or users. Multi-layered security technologies - including system hardening, exploit prevention, file integrity monitoring, network attack blocking and static & behavioral anti-malware - deliver comprehensive protection throughout the entire infrastructure, from virtualized servers and desktops to public cloud (AWS, Azure, Google Cloud) instances.
* Industrial Cybsersecurity – Kaspersky Industrial Cybersecurity is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMI, engineering workstations, PLCs, network connections and people – without having an impact on operational continuity and the consistency of industrial processes.
* Automated Security Awareness services offer a new approach to online educational programs. Simplified objective-setting, automated learning paths, practical exercises based on real-life scenarios all help in delivering effective results and a successful outcome, for participants and training management alike.

The Group also extends its product portfolio in portfolio in Security Services (Managed Detection and Response, Threat Hunting, Security Assessment), Anti-DDoS Protection, Online Fraud Prevention, Anti-Targeted Attacks, EDR (Endpoint Detection & Response), and Embedded Systems Security).

The Group’s revenue increased by 6% from USD 713 million in 2020 to USD 758 million in the current reporting period. Revenue in constant currency terms increased in 2021 by 6.7% compared to 2020.

The Group’s profit from operating activities decreased by 55% from USD 110 million in 2020 to USD 49 million in 2021, the decline mainly being due to increase of employee compensation, which reflects the Group’s determination to invest in people.

The Group’s EBITDA[[1]](#footnote-1) decreased from USD 161 million in 2020 to USD 102 million in 2021. Its dynamics corresponds to the change in operating profit.

The Group’s net finance costs of USD 11 million (2020: costs of USD 24 million) decreased compared 2020 due to a net foreign exchange gain of USD 20 million, which is partially offset by a higher impairment of loans receivable from an associate and a third party.

The Group’s profit before income tax decreased by 56% from USD 87 million in 2020 to USD 38 million in the current reporting period.

The Group’s effective tax rate decreased from 75% in 2020 to 63% in 2021 mainly due to a lower effect of changes in tax rates in foreign jurisdictions. The group’s effective tax rate for 2020 reported in the consolidated financial statements as at and for the year ended 31 December 2020 (53%) was adjusted in the preparation of these consolidated financial statements for comparability due to an amendment of the methodology for calculating deferred tax on deductible temporary differences arising from contract liabilities. Refer for details to Note 35 to the consolidated financial statements.

As a result of factors described above, the Group’s net profit for 2021 amounted to USD 14 million.

**Statement by the Directors in performance of their statutory duties in accordance with s172 Companies Act 2006**

The Directors consider the following issues, factors and stakeholders relevant in complying with section 172 (1) (a) to (f):

Regard to the likely consequences of decisions in the long term

The 2022 budget which was approved in 2021 places focus on the Group’s profitability, which is meant to be achieved through a combination of revenue growth and efficient spending in strategically important directions.

Regard to the interests of the company’s employees

Employee remuneration is reviewed on an annual basis to ensure that it is at a fair market level. Employee remuneration amounted in 2021 to 62% of the Group’s operating expenses (2020: 57%). Employee involvement and commitment to the success of the business is an important element of the Company’s culture. Management conducts regular communications and consultations with employees on key aspects of the Company’s activities in the form of e-mail communications, annual meetings and informal events. A significant portion of employees bonuses depend on the financial performance of the business unit that they belong to and/or Kaspersky Group as a whole. An annual review of employee compensation is performed to support the business strategy of profitable revenue growth, which should in turn provide interesting and fulfilling work and the prospect of a higher future remuneration if the strategy is successfully achieved. The Group hiring policies stipulate full and fair consideration to applications for employment made by disabled persons, having regard to their particular aptitudes and abilities. We provide continuing employment to those employees who become disabled during their employment with the Group, and provide training, career development and promotion to disabled employees, where appropriate.

Regard to the need to foster the company’s business relationships with suppliers, customers and others

The Board is committed to ensure that the Group strictly comply with its obligations to its suppliers and customers. The Company reports it’s commitment to its customers through providing them top quality products.

Regards to the impact of the company’s operations on the community and the environment

The Group is conscious of its environmental responsibilities and aims at reducing any damage to the environment that might be caused by its activities, primarily by reducing energy consumption.

UK Greenhouse gas emissions and energy use data for the period 1 January 2021 to 31 December 2021:

|  | **2021** |  | **2020** |
| --- | --- | --- | --- |
| **Energy consumption used to calculate emissions (kWh)** | 115,095.47 |  |  116,673.96  |
| **Energy consumption break down (kWh):** |  |  |  |
| • gas |  1,662.60  |  |  2,474.92  |
| • electricity |  105,432.10  |  |  77,077.00  |
| • transport fuel |  8,000.77  |  |  37,122.05  |
| **Scope 1 emissions in metric tonnes CO2e** |  0.30  |  |  0.46  |
| Gas consumption |  0.30  |  |  0.46  |
| **Scope 2 emissions in metric tonnes CO2e** |  **22.39**  |  |  **17.97**  |
| Purchased electricity |  22.39  |  |  17.97  |
| **Scope 3 emissions in metric tonnes CO2e** |  **2.24**  |  |  **10.41**  |
| Business travel in employee owned vehicles |  2.24  |  |  10.41  |
| **Total gross emissions in metric tonnes CO2e** |  **24.93**  |  |  **28.84**  |
| **Intensity ratio Tonnes CO2e per employees**  |  **0.25**  |  |  **0.26**  |

Quantification and reporting methodology

We have followed the 2019 HM Government Environmental Reporting Guidelines. We have also used the GHG Reporting Protocol – Corporate Standard and have used the 2020 UK Government's Conversion Factors for Company Reporting.

Intensity measurement

The chosen intensity measurement ratio is total gross emissions in metric tonnes CO2e per average number of people employed during 2021 and 2020.

Measures taken to improve energy efficiency

Most of energy and carbon is consumed by the Group as office or travel expenses. Due to COVID-19 pandemic most of the Group’s employees worked from home during the reporting period and business travel activity reduced to a minimum. This allowed to achieve a low energy consumption during 2021. While this was not a result of conscious measures taken to improve energy efficiency, this allowed to accumulate resources for energy efficiency measures for the future periods.

Regards to the desirability of the company maintaining a reputation for high standards of business conduct

The Board considers that the reputation for high standards of business conduct derives primarily from meeting its obligations to its customers and suppliers, involving employees in the relevant areas of its business activity and promoting cybersecurity to make the world safer.

Regards to the need to act fairly as between members of the company

The Group treats all its shareholders fairly and no preferences are made to some shareholders at the expense of the others. During 2021 the Group declared dividends of USD 11,000 thousand (2020: no dividends declared) and did not enter in material transactions with any of its members, apart from the fact that some of the Group’s shareholders are part of the management and/or are employed by the Group.

**Corporate Governance Report**

The Group does not apply a formal corporate governance code. All the entities inside the Group are governed in accordance with the relevant laws and constitution and by-laws that apply in their country.

The key members of the Company are the Company’s Board of Directors. The nature and functions of the Board and the manner in which it is conducted is aligned with the Articles and Memorandum of Association of the Company. All the Company’s Directors are equally involved in managing all sides of the Company’s activities and interact with the members of the Company in accordance with the laws of the UK.

There is no governance code required because the management of the Company and the Group management on the highest level is executed by the same permanent group of chief managers, headed by major beneficial owners (members) of the Group, in the form of the Company’s Board of Directors. In this respect the Company has no practical need for any special governance code or supplementary arrangements for corporate governance as the Board and the shareholders are structurally aligned.

DETAILED FINANCE AND LEGAL INFORMATION ABOUT KASPERSKY LABS LIMITED CAN BE FOUND AT https://www.gov.uk/government/organisations/companies-house

1. EBITDA for twelve months ended 31 December 2021 includes IFRS operating profit of USD 49 million (2020: USD 110 million) plus depreciation and amortisation USD 53 million (2020: USD 51 million). [↑](#footnote-ref-1)