Kaspersky modern slavery policy

kaspersky BRING ON THE FUTURE

Learn more:
kaspersky.com

Introduction

This statement is issued by Kaspersky under the provisions of the Modern Slavery Act 2015. This statement sets out Kaspersky Labs Limited (the Company) and related Kaspersky Group companies (the Group) actions to understand all potential modern slavery risks related to its business and to put in place steps that are aimed at ensuring that there is no slavery or human trafficking in its own business and its supply chains.

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".

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. 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. As part of IT industry, we recognise that we have a responsibility to take a robust approach to slavery and human trafficking and we continue to take our responsibility very seriously during the coronavirus pandemic.

Our organisation is absolutely committed to preventing slavery and human trafficking in its corporate activities, and to ensuring that its supply chains are free from slavery and human trafficking.

Organizational structure and supply chains. Countries of operation and supply

The principal activity of the Company is antimalware software development, marketing and distribution of information security solutions by Kaspersky, which protect its customers from a wide range of IT threats, including viruses and other forms of malicious software, spam, hackers, intrusions, and unauthorized use or disclosure of confidential information.

Relevant business, back-office, R'n'D and technical support departments of Kaspersky maintain business activities of the Company all over the world.

Kaspersky strictly complies with its obligations to its suppliers and customers by the Company's commitment to its customers through providing them top quality products. The Group undertakes research and development in connection with its principal activity.

Kaspersky 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 mediumsized businesses to large governmental and commercial organizations.

Kaspersky'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.

The key market in which Kaspersky operates is endpoint security. It encompasses products that are designed to protect endpoints from attack or to protect information residing on endpoints, both physical and virtual, regardless of operating system type. Endpoint security products provide security using or leveraging an endpoint agent or client as a core or fundamental component. Functionality includes client antimalware software, file/storage server antimalware, personal firewall software, host intrusion prevention software, file/disk encryption, whitelisting, patch management, desktop URL filtering and endpoint data loss prevention.

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 Company 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. Kaspersky'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.

Our customers are from different industries of wide range, Kaspersky products can be implemented for production industries, finance and deep technology companies, huge national and international companies, small and medium business and of course are widely used by end customers to protect their PCs and mobile devices from malicious software.

The Group conducts operations on different national markets and can be significantly affected by geopolitical situations in the world. To cope with these geopolitical challenges the Group abides by the highest ethical business practices, and through its Global Transparency Initiative launched in 2017, it is exemplifying its ongoing commitment to assuring the integrity and trustworthiness of its products.

The Group operates in a market where technology plays a key role. Maintaining industry leadership positions is subject to a number of risks. Specifically, the Group may lack financial and other resources to maintain its positions. Products in the Group's target market are technologically complex and vulnerable to defects and error. Additionally, a possible infringement of the Group's intellectual property rights may negatively affect the Group's competitiveness in the market.

The Group manages this risk by investing substantial resources in research and development activities, including those which are related to ensuring product quality, as well as in legal substantiation of its intellectual property rights.

Interests of employees

The Company is the employer of the highest commitment and liability towards its employees. As a company operating in the sphere of IT-business, which is known for its high standards of employment protection and employees profits provision, Kaspersky's activities do not relate any hazardous employment and the Company does not execute any activities that considered to be at high risk of slavery or human trafficking.

Employee remuneration is reviewed on an annual basis to ensure that it is at a fair market level. Employee remuneration amounted in 2020 to 57% of the Group's operating expenses.

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.

Responsibility for our anti-slavery initiatives is as follows: we operate the following policies that describe our approach to the identification of modern slavery risks and steps to be taken to prevent slavery and human trafficking in its operations:

Whistleblowing policy

We encourage all our workers, customers and other business partners to report any concerns related to the direct activities, or the supply chains of, our organisation. This includes any circumstances that may give rise to an enhanced risk of slavery or human trafficking. Our whistleblowing procedure is designed to make it easy for workers to make disclosures, without fear of retaliation. Employees, customers or others who have concerns can appeal to specially appointed officers of the Company.

Anti-bribery policy

The Company stands for independent and reasoned choice of its suppliers and partners made in accordance with due diligence of high standards. By implementation of anti-bribery policy, Kaspersky requires from its supplier chain manager to follow clear procurement procedures, which do not allow having any corruption element.

Sanction Compliance policy

The aim of Sanction Compliance is to ensure compliance of the Group's activities with sanctions programs imposed by monitored jurisdictions. All employees, suppliers and partners of Kaspersky Labs entities are subject of the sanction compliance policy. The Group follows a risk-based approach to sanction compliance by developing, implementing and regularly updating Sanction Compliance Procedures in order to manage the sanction risk in the Group's operations.The Group follows a zero tolerance to sanction risk violations and tends to compliance with all sanction regulation, applicable for the jurisdiction of the Group's office. All the information on sanction compliance checks, sanction statuses of the counterparties, sanctions policy violations and black lists of companies and individuals is stored in the Sanction Compliance IT system.

The Group follows a risk-based approach to any sanction compliance by developing, implementing and regularly updating Sanction Compliance Procedures in order to manage the sanction risk in the Group's operations. The Group tends to comply with all sanction regulation, applicable for the jurisdiction of the Group's office.

The Group does not engage or does not accept any activity that does not comply with corporate sanction compliance rules. Inconsistent interpretations of sanctions legislation ought to be considered by sanction compliance managers separately with involvement of responsible employees, able to provide required expertise.

Employees of the Companies of Kaspersky Group, understanding that sanctions can potentially be imposed against members of the management bodies of the Companies and related persons, seek to reduce the associated risks, using the Sanctions Compliance Procedures.

The Group continuously monitors all changes in all applicable legislation and their practice of application. Kaspersky employees and representatives are prohibited from mediating and concluding transactions with third parties if this event causes the realization of sanctions risk.

All the information on sanction compliance checks, sanction statuses of the counterparties, sanctions policy violations and black lists of companies is stored in the Sanction Compliance IT system also named as Sanction Compliance Software. The IT resource is owned by Kaspersky compliance managers who are responsible for keeping the data up to date, providing availability of the resource and access right regulation.

Employee Handbook

Our employee handbook makes clear to employees the actions and behaviour expected of them when representing our organisation. We strive to maintain the highest standards of employee conduct and ethical behaviour when operating abroad and managing its supply chain. Employee handbook gives a wide and detailed overview of ethic policy implemented in the Company and provides the clear behaviour guidance for all the employees to prevent any discrimination and harassment. Kaspersky's employees are made aware of their employment rights through a variety of channels, including written employment contracts and policies, and procedures found in employee handbook and staff websites.

Supplier/Procurement policy

We are committed to ensuring that our suppliers and partners adhere to the highest standards of ethics and laws conduct. Under the Company's due diligence policy suppliers are required to demonstrate their highest level of laws observation including but not limited to treatment of workers with dignity and respect and acting. We work with suppliers to ensure that they meet the standards of the code and improve their worker's working conditions.
The particularity of our business allows cooperating with highly reliable large companies whose reputation is unquestionable.
The business of the Group does not require any supplement which can be bound with men slavery or human rights infringement that may from time to time happens in undeveloped countries. The main asset of Kaspersky is intellectual property produced by Kaspersky's employees. Due to specialty of software business Kaspersky does not require being supplied with any hazard substances, metals, heavy industry goods, etc. Kaspersky's supplement chain does not base on products or services of industries where inhuman working conditions may take place.

A particular risk of encountering modern slavery for us lies in spheres where we do not have direct management control. But due diligence of law risk approach executed by Kaspersky in respect of every and any supplier and following procurement policies and procedures reduces the risk to zero.

Our approach covers our business's purchasing practices, which influence supply chain conditions and which should therefore be designed to prevent purchases at unrealistically low prices, the use of labour engaged on unrealistically low wages or wages below a country's national minimum wage, or the provision of products by an unrealistic deadline.

Due Diligence and Risk assessment

We undertakes due diligence when considering taking on new suppliers or partners, and regularly reviews its existing suppliers. Our due diligence and reviews include mapping the supply chain broadly to assess particular product or geographical risks, reviewing on a regular basis all aspects of the supply chain based on the supply chain mapping; conducting supplier audits or assessments through the organisation's own staff, creating a risk profile for each supplier; invoking sanctions against suppliers that fail to improve their performance in line with an action plan or seriously violate our supplier code of conduct, including the termination of the business relationship.

Our risk assessment indicators are: developing a system for supply chain verification whereby we evaluate potential suppliers before they enter the supply chain; and reviewing its existing supply chains, whereby we evaluate all existing suppliers.

Recruitment policy

We use only specified, reputable employment agencies to source labour and always verifies the practices of any new agency it is using before accepting workers from that agency. Every new employee is verified for good employment and legal history including the receipt of former employees' references.
The same approach we use when engage for outsource

Trainings

We arrange duly informing all staff and especially HR professionals within our organisation on human rights and ethics training programmes.
We require supply chain managers to follow due diligence procedures in respect of partners to be every time sure that none of them breaches the applicable laws.

Kaspersky independently or with the assistance of third-party specialists in the field of legal compliance implements and supports the training program for all employees and develops a training system and maintains up-to-date training materials.

All Group employees are required to get familiar with the procedures under the compliance policies and procedures.

Employees rights observation during COVID-19 pandemic

The company has considered the impact of the COVID–19 pandemic on the situation with slavery monitoring and employees protection inside the Group and in its operations and supply chains. Kaspersky has commissioned internal research on the potential impact of the pandemic on the employees within the company, and come to a conclusion that COVID -19 did not aggravate a situation with employees' rights observation. The company's management of the highest and local levels implemented all possible measures to protect employees from risks of catching COVID- 19 disease, which includes among others: providing employees with the possibility to work from home, moving employees to the distanceworking regime, making trainings about working and living within COVID-19 pandemic and advantages of duly vaccination, arranging day-to-day working regime of company's offices in a strict accordance with medical, sanitary and legal requirements of relevant countries, monitoring of situation with employees caught the disease and providing them paid sick leaves and applicable medical services.

Because of sensitivity related to personal data and GDPR regulations Kaspersky has no opportunity to check how pandemic situation affected its partners and suppliers. However, it's common legal compliance monitoring processed in respect to its suppliers has not shown any improprieties in this area.

Based on these assessments and considerable resources of the Group spent to maintain health and normal work of its employees together with long-standing relationships with a number of customers and suppliers across different geographic areas and industries, Kaspersky believes that the Group is well placed to manage its COVID-19 risks successfully.

As of the date of this report, the effect of the pandemic has not been significant for the Group. Management cannot currently reliably estimate the influence of COVID-19 on the Group's future performance, but are confident that the outbreak of the virus does not raise a going concern question for Kaspersky.

This statement was approved on 13th January, 2022 by Kaspersky Labs Limited board of directors.

For and on behalf of the Board
Svetlana Ivanova,
Director and Secretary

kaspersky.com

kaspersky

GBD-9078 Q1/22 V1