Managing ESG risks

Kaspersky's senior executives and department heads are responsible for managing the Company's sustainability risks. During the reporting period, Kaspersky identified three key ESG risks: changes in the political and economic sphere as well as legislation in the regions of the Company's presence, rise in cybercrime and supply chain disruptions.

Key ESG risks

Risk	Why the risk is important	Risk management measures in 2022 and 2023
Changes in the political and economic sphere as well as legislation in the regions of the Company's presence	Possible changes in legislation could significantly limit the Company's ability to do business in the country/region of presence.	■ Regular monitoring of changes to legislation in the countries/regions where the Company operates in order to promptly identify potential risks. ■ Membership of the Company and its experts in various industry organizations to take part in communications with the regulatory authorities. ■ Participation in public consultations held by the government authorities in countries/regions where the Company operates on projects to amend existing regulations or introduce new ones in order to promote the Company's position. ■ Further development of the Global Transparency Initiative (GTI) in order to verify the reliability of the Company and its products for corporate customers, partners and regulators.
Rise in cybercrime	The level of cooperation between law enforcement agencies and private companies in different countries is diminishing in the current environment. To prevent a surge in cybercrime, it is crucial to maintain cooperation and exchange expertise with the private sector.	The Company continued to actively cooperate with law enforcement agencies and international organizations during the reporting period: ■ Assisted INTERPOL in conducting operations Africa Cyber Surge in November 2022 and Africa Cyber Surge II in August 2023, aimed at disrupting and combating cybercrime in African countries. ■ Organized training on incident response and malware analysis for more than 100 representatives of law enforcement agencies from various countries under the auspices of INTERPOL. ■ Took part in the INTERPOL International Cybersecurity Conference. ■ Participated in preparing feedback and proposals for the draft Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which is currently being developed under the auspices of the UN. ■ Signed memorandums of understanding with several national regulators in the field of cybersecurity.
Supply chain disruptions	Geopolitical changes could cause disruptions in supply chains and have a negative impact on the Company's business and performance.	We ranked our services based on the level of their importance to business continuity and impact on results. Even though we assess the risk of supply chain disruptions as low, we have undertaken measures to mitigate this and switch to using new services and platforms, including: ■ Phasing out imports of software, systems, equipment and services. – Transition from CRM Sales Force to the Russian Bitrix platform. – Purchase of equipment from a Russian certified vendor. ■ Modifying logistics for the procurement of key components and replacing suppliers who were unable to provide equipment, software and services or were not willing to continue cooperation. ■ Transferring technical support and infrastructure services to other regions of the world.