TRANSPARENCY AND RESPONSIBILITY REPORT 2023

Contents

A Message from the CEO

December 31, 2023

On October 7, 2023, Hamas terrorists infiltrated Israel and launched a horrendous attack on innocent civilians. More than 1,200 people were massacred, at least 3,000 were wounded, and over 240 were kidnapped to the Gaza strip during these deadly raids. The "success" of terror attacks like these were often facilitated by the use of end-to-end encryption applications which are used by terror organizations as a primary means for planning and executing attacks.[1] *This serves as a singular example demonstrating the urgency and critical necessity of cyber intelligence technologies.*

At NSO Group, our mission is clear and simple. We help government intelligence and law enforcement agencies lawfully address their most pressing national security and public safety issues. Our best-in-class cyber intelligence products have been and are used to prevent terrorism, counter serious crime, break up pedophilia-, sex-, and drug-trafficking rings, find and rescue kidnapped children, and locate survivors of natural disasters. NSO Group was founded to make the world a safer and more secure place, and we continue to work towards this goal.

In 2021, we published our first Transparency and Responsibility Report to share who we are, what we do, and how we approach and embrace our responsibility to conduct business in an ethical manner and uphold human rights to the fullest extent. Today, through the release of our second Transparency and Responsibility Report, we hope to demonstrate our deep and ongoing commitment to hold ourselves to the highest ethical standards, inspire others in the cyber intelligence industry to come forward to explain their own corporate ethos and processes, and invite stakeholders to engage in informed and constructive dialogue regarding the responsible development, sale, and use of cyber intelligence technology.

Cyber intelligence technology is a critical tool for preventing and investigating terrorism and serious crimes, and for thereby protecting individuals' fundamental rights to life, liberty, and security. The need for and importance of cyber intelligence technology has been once again highlighted by the recent events in Israel and their aftermath

Effective and timely intelligence support is crucial in detecting and disrupting terror acts against innocent civilians. Since the October 7 terror attack, we have seen a surge in terrorism and antisemitic attacks, and as we anticipate an increase in similarly grave acts on a global scale, our clients are emphasizing the imperative need for efficient tools to counter threats of terrorism. Just recently, we witnessed multiple terrorist attacks in major Western European cities, indicating imminent security threats. As a response to the rise in terrorism, The European Union and national security agencies are in discussions regarding on the necessity to expose terror actors going dark, and the importance of countering the misuse of end-to-end encrypted communication technology.[2] *Cyber intelligence technology enables government intelligence and law enforcement agencies to carry out their basic duties to prevent violence and safeguard the public. Importantly, it allows them to counter the widespread deployment of end-to-end encryption applications by terrorists and criminals without engaging in mass surveillance or obtaining backdoor access to the devices of all users.*

However, like any other technology, cyber intelligence technology can also be misused or abused to violate other important human rights, such as the rights to privacy and free expression. As a company, NSO Group recognized early on—and has taken concrete steps to address—potential downstream human rights impact of our products. As detailed in our previous report, this included the development and implementation of a comprehensive, industry-leading human rights compliance program, which has now been in operation for nearly four years.

As evident from this comprehensive report, there has been a significant decrease in reports of product misuse during 2022 and 2023, a result attributed to our diligent compliance activities and efforts. Throughout 2022 and 2023, we have continued to uphold and improve our processes designed to prevent human rights abuses, and sought opportunities to make additional enhancements to our overall human rights compliance program. As outlined in this report, we have strengthened our human rights due diligence process, increased

---

[1] *See* Center for Strategic and International Studies, *Understanding Hamas's and Hezbollah's Uses of Information Technology* (July 31, 2023), https://www.csis.org/analysis/understanding-hamass-and-hezbollahs-uses-information-technology.

[2] *See* Matthew Dalton, The Wall Street Journal, *Europe Faces New Terrorism Threat Fueled by Israel-Hamas War* (December 5, 2023), https://www.wsj.com/world/europe/europe-faces-new-terrorism-threat-fueled-by-israel-hamas-war-12ecc4dd.

contractual obligations of our customers, developed and distributed further guidance on the proper use of our products,

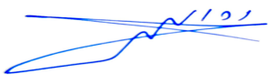
and investigated and even terminated customers who failed to meet our compliance expectations, and contractual obligations. We have also undertaken initiatives to study the potential impact of our products on journalists, designed technological safeguards to help mitigate the risk that our customers might misuse our products, and engaged with regulators regarding an international framework governing the development, sale, and use of cyber intelligence technology. These efforts are a result of our unwavering commitment to ethical and responsible business conduct, and I am deeply grateful to our employees and shareholders who share NSO Group's vision to provide products that help prevent and investigate terrorism and serious crimes, and that are used safely and responsibly in accordance with applicable domestic and international laws and ethical norms.

Notwithstanding the fact that our products play a crucial role in saving lives and ensuring global safety, as our clients constantly inform us, we fully understand that our processes are not perfect and may not always prevent government end users of our products from acting in contravention of their contractual and ethical obligations to only operate our products in accordance with international norms. By publishing updates regarding our processes and practices, we hope to create more opportunities for honest feedback, dialogue, and continuous improvement. We also remain optimistic that this report can help further drive and meaningfully contribute to building a global framework for regulation of cyber intelligence technology.

Balancing competing rights and interests in today's dynamic world requires close collaboration among all stakeholders. On one hand, we are confronted with wars, terrorist attacks, and serious crimes that threaten national security and the physical safety of innocent civilians. On the other, we have the important responsibility to respect all human rights and fundamental freedoms, including the rights to privacy and free expression. Protecting human rights while countering terrorism is a nuanced and challenging endeavor, but it is something that we must continue to strive to do in order to make the world a safer place for all.

With these goals and aspirations in mind, it is my honor to present NSO Group's second Transparency and Responsibility report.

Sincerely,



Yaron Shohat
Chief Executive Officer
NSO Group

Executive Summary

NSO Group's 2023 Transparency and Responsibility Report provides essential information about the company's continued commitment to human rights, ethics, and corporate responsibility. It reflects our activities and learnings over the past two and a half years, as well as our future goals and aspirations. In providing this report, we are constrained in our ability to share certain details due to factors that are unique to our industry, including strict confidentiality requirements of our customers given their highly sensitive intelligence and law enforcement activities. Our capacity for action is also limited by the fact that we do not operate our products, nor have any real-time visibility or influence with respect to the particular individuals investigated by our government customers using our products. Nevertheless, this report contains key insights into how we carry out our mission to help prevent and investigate terrorism and serious crimes in support of our government customers' duties to protect their citizens from physical harm, while balancing—and striving to minimize—the potential for misuse of our products that could adversely impact individuals' rights to privacy and free expression, among other human rights.

This report is divided into four sections. First, we provide an overview of who we are and what we do as a company. While we develop and license a number of technology-based products, we are most well-known for our "Pegasus" system, which is a cyber intelligence tool used by legitimate intelligence and law enforcement agencies of sovereign states to prevent and investigate terrorism and serious crimes. Although an overwhelming media spotlight has been cast on our Pegasus technology over the past several years, it remains poorly understood. This report thus attempts to dispel falsehoods, explain what Pegasus does, and, just as importantly, what it does not. Second, we outline our current approach to human rights, drawing particular attention to our human rights compliance program, including recent updates and related improvements to our processes. We describe the policy framework and the ways in which the various components of our commitment to respect human rights are implemented throughout our business. Third, we additionally highlight certain notable developments regarding our efforts to protect and promote human rights during 2022 and 2023. These include a focused impact assessment on journalists, heightened due diligence and oversight, enhanced guidance for elevated-risk customers, cooperation with external inquiries, and engagement with stakeholders regarding the development of an international framework for regulating the sale and use of cyber intelligence technology. Finally, we identify a number of goals for further enhancement of our human rights compliance efforts.

As a provider of cyber intelligence technology, with a goal of providing life-saving products to our clients, we nevertheless recognize that there are serious potential risks that could be associated with misuse of our products, including potential adverse impacts on human rights. We have taken—and will continue to take—concrete steps to address, prevent, and mitigate risks of product misuse. By detailing our existing processes and plans for enhancements in this report, we hope to receive constructive feedback from stakeholders and create opportunities for continued dialogue and engagement. We remain motivated to learn and improve our processes, and continue to set industry standards for responsibly supplying cyber intelligence technology to help governments combat terrorism and serious crimes.

Understanding Pegasus

- **Pegasus is not a mass surveillance tool.** It is used with specific, pre-identified phone numbers of suspected terrorists and criminals, one at a time. In many ways, Pegasus is similar to a traditional wiretap.
- **Pegasus is not operated by NSO Group.** It is licensed to legitimate, vetted intelligence and law enforcement agencies of sovereign states for prevention and investigation of terrorism and other serious crimes in accordance with applicable laws and regulations.
- **Pegasus cannot take control of a device, manipulate existing data, or implant new information.** It is technologically impossible for Pegasus to add, alter, delete, or otherwise manipulate data on targeted mobile devices, or perform any other activities beyond viewing and/or extracting certain data.
- **Pegasus does not penetrate computer networks, desktop or laptop operating systems, or data networks.** It can be installed only on smartphones and cannot be used to gather information more broadly.

About NSO Group

NSO Group, founded in 2010, is a global technology company based in Herzliya, Israel. We develop and license cyber intelligence tools and other technology-based solutions to help government authorities and law enforcement agencies detect, prevent, and investigate terrorism, serious crimes, and other major challenges to public safety.

Our Mission

At NSO Group, we are dedicated to providing government agencies with the best-in-class cyber intelligence tools. The goal here is clear and simple—to make the world a safer place – a prime objective outlined in Goal 16 of the United Nations Sustainable Development Goals. Terrorist organizations, organized crime groups, drug cartels, human traffickers, pedophile rings, and other criminal syndicates continue to exploit off-the-shelf encryption capabilities offered by mobile messaging and communications applications. These applications provide terrorists and criminals a safe haven, allowing them to "go dark" and secretly plan, plot, and conspire to commit unlawful activities. Our products are designed to counter the growing misuse of end-to-end encryption applications by terrorists and criminals and enable government and law enforcement agencies to carry out their duty to protect citizens from violence and criminal activity, thus promoting the achievement of Goal 16 objectives – reducing all forms of violence and progressing towards peaceful and inclusive societies.

The "Going Dark" Problem

Governments around the world are struggling to keep pace with technological advancements that restrict their ability to successfully prosecute cases or timely detect threats to national security and public safety. According to the former FBI Director "Going Dark" means when those charged with protecting citizens "have the legal authority to intercept and access communications and information pursuant to court order," but "lack the technical ability to do so."

Indeed, as individuals became increasingly reliant on smartphones, technology companies and application developers began to develop encryption capabilities in an effort to ensure privacy and protect personal information. Chief among these is end-to-end encryption, which allows messages or data to be securely transmitted from one user's device to another's without being intercepted and reviewed by third parties, including law enforcement.

While end-to-end encryption greatly benefits law-abiding citizens who seek to protect their information from malicious hackers, it also poses grave security threats as terrorists and criminals are able to use the same technology to plot attacks and facilitate crimes. Indeed, there is ample evidence that perpetrators of terrorist attacks have repeatedly exploited encrypted mobile communications to evade detection by law enforcement.

Our Values

In working towards our goal of making the world a safer place, NSO Group is guided by our four core corporate values—accountability, excellence, integrity, and boldness. Taken together, these values form the foundation of our company culture, serve as our moral compass, and guide our decision-making.

ACCOUNTABILITY

We apply rigorous ethical standards to everything we do. Our customers vetting methodology includes a strict licensing process from the relevant export control authority, as well as a structured, in-depth human rights due diligence review.

INTEGRITY

We are committed to the proper use of our products – to help government agencies protect their citizens against terror, crime and other major security threats. We take this commitment seriously and investigate any credible allegation of product misuse.

EXCELLENCE

We are committed to providing government agencies with best-in-class cyber intelligence technology and related services. We have a track record of success, and our products have been used to save thousands of lives.

BOLDNESS

We believe success comes from being intrepid. At NSO Group, we emphasize being bold yet accountable. We continuously seek innovative ways to make our products more effective, safe and responsible.

Our Leadership

NSO Group's leaders are entrusted with instituting our ethical standards, culture, and values. As discussed in more detail later in this report, our Board of Directors, through the advice and support of the Governance, Risk, and Compliance Committee ("GRCC"), is responsible for overseeing the implementation of company policies and procedures, including the Code of Ethics and Conduct and Human Rights Policy. Our Management Committee, which is comprised of the Chief Executive Officer ("CEO"), Senior Vice President of Client Business Division ("SVP Business"), and General Counsel ("GC"), is in charge of ensuring that the company's processes are being followed and functioning effectively in our day-to-day operations.

Our Products

As a technology company, we provide a suite of products designed to save lives and protect public infrastructure. We develop and license cyber intelligence solutions that help legitimate intelligence and law enforcement agencies lawfully infiltrate mobile devices of specific suspected terrorists and criminals. In addition, we offer geolocation tools that are used for search-and-rescue missions.

We are, however, most well-known for "Pegasus," a system used by select licensed and vetted government agencies to surveil and collect data from mobile devices of particular individuals suspected of engaging in terrorist or criminal activity. While substantial public attention has been drawn to Pegasus over the years, the technology remains poorly understood. First and foremost, Pegasus is not a mass surveillance tool. Instead, it can only be used with specific, pre-identified phone numbers of suspected terrorists and criminals, one at a time. The Pegasus system allows for targeted surveillance only, with customers purchasing a license that defines and limits the number of permissible installations within a given period. In many ways, Pegasus is similar to a traditional wiretap. By enabling law enforcement authorities to monitor, for a defined period of time, mobile communications of specific individuals suspected of participating in terrorism or crime, Pegasus offers authorized government personnel a narrow window into the activities of previously identified, suspected criminal actors on an individual basis.

To be clear, NSO Group does not operate Pegasus, nor do we have any knowledge about the individuals whom our government customers might be investigating or the plots they are trying to disrupt as part of their highly confidential intelligence and law enforcement operations. Our role is strictly limited to developing and licensing the Pegasus technology to legitimate intelligence and law enforcement agencies, and providing related technical support and maintenance services for the duration of the relevant contract period. Indeed, the Pegasus system is configured with multiple separated compartments that provide technological blocks so that unauthorized parties cannot access user interface logs or data extracted from targeted devices. Governments do not and should not share any information about their investigative activities with NSO Group or any other provider of similar technology.

> Pegasus recently enabled us to access the devices of IS supporters involved in setting up a terror cell. A coordinated operation with our partner agencies led us to prevent preparations for attacks, saving many lives. Additionally, crucial intelligence was gathered from the target device using Pegasus leading to earlier arrests than anticipated; otherwise, a major suspect would have escaped (Western European client, May 2023).

Contrary to certain allegations, Pegasus cannot add, alter, delete, or otherwise manipulate data on targeted devices. It is technologically impossible for Pegasus to perform any other activities beyond viewing and collecting data on targeted devices. Moreover, Pegasus can be installed only on smartphones and cannot be used to gather information more broadly—it does not penetrate computer networks, desktop or laptop operating systems, or data networks.

In fact, Pegasus is treated as a "defense article," meaning that the technology is subject to strict export control laws. For example, NSO Group is required to obtain marketing and export licenses from the Israeli Ministry of Defense's Defense Exports Control Agency ("DECA") in order to engage in any sales discussions regarding Pegasus and ultimately complete its sale. DECA exercises close regulatory oversight over companies in our industry, conducts its own monitoring and assessments of human rights risks in countries across the world, and requires importing governments to sign an end-user declaration[3] addressed to the Israeli Ministry of Defense as a condition to obtain their licenses, among other measures.

Pegasus is subject to strict regulatory oversight from export control authorities who conduct their own assessments of human rights risks.

Pegasus has been used by government agencies to address serious crimes and save lives on a massive scale. With our technology, intelligence and law enforcement authorities around the world have thwarted numerous terrorist attacks, captured and brought pedophiles to justice, broken up criminal organizations and drug trafficking rings, and freed kidnapping and human trafficking victims. Yet, the highly sensitive and confidential nature of intelligence and law enforcement operations of sovereign governments prevent publication of details related to these "success stories." This creates significant information asymmetry between the benefits derived from the use of Pegasus and the potential adverse impacts associated with its misuse. Pegasus is nonetheless a crucial tool for intelligence and law enforcement agencies. On numerous unreported occasions, Pegasus has contributed to the fight against terrorism and serious crimes and, therefore, to the protection of the fundamental rights of individuals.

[3] State of Israel Ministry of Defense, Defense Export Control Agency, *End Use/User Certificate* (January 2023), available at https://exportctrl.mod.gov.il/Documents/%D7%94%D7%A6%D7%94%D7%A8%D7%94%20%D7%A1%D7%99%D7%99%D7%91%D7%A8.pdf.

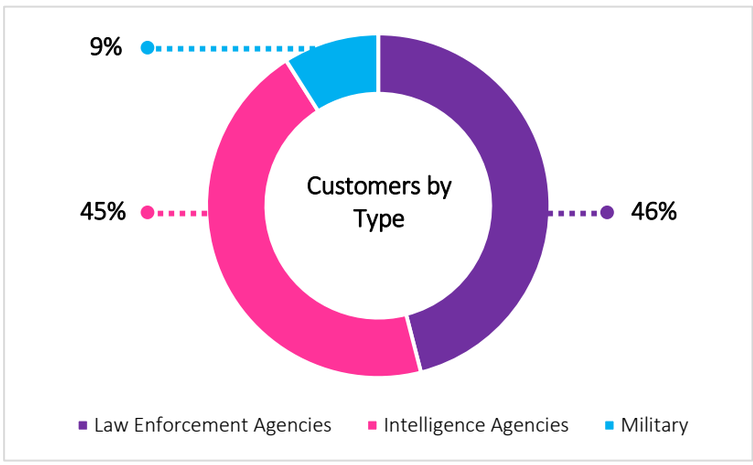
Rights We Seek to Protect

- **Right to Life,** Universal Declaration of Human Rights ("UDHR") Article 3; International Covenant on Civil and Political Rights ("ICCPR") Article 6
- **Right to Liberty and Security,** UDHR Article 3; ICCPR Article 9
- **Right Not to Be Held in Slavery or Servitude,** UDHR Article 4; ICCPR Article 8
- **Right Not to Be Subjected to Torture or to Cruel, Inhuman, or Degrading Treatment or Punishment,** UDHR Article 5; ICCPR Article 7
- **Right Not to Be Subjected to Arbitrary Arrest or Detention,** UDHR Article 9; ICCPR Article 9
- **Right to Liberty of Movement and Freedom to Choose Residence,** UDHR Article 13; ICCPR Article 12

56 customers

IN

31 countries



Approach to Human Rights

As a company, NSO Group is firmly committed to respecting all human rights, as enshrined in the International Bill of Human Rights. In doing so, we are guided by the authoritative international standards articulated in the United Nations Guiding Principles on Business and Human Rights ("UNGPs"), the Organisation for Economic Co-operation and Development Guidelines for Multinational Enterprises, and the United Nations' Counter Terrorism Legal Training Curriculum. We have implemented our commitment to uphold human rights through a comprehensive, industry-leading human rights-focused compliance program. Developed in consultation with leading business and human rights experts, our framework codifies NSO Group's core values, beliefs, and expectations about how we ought to carry out our business and conduct ourselves in all aspects of our work—from the design and development to the licensing and distribution of our products. We similarly expect and demand our business partners and customers to respect human rights in accordance with international standards and norms.

We fully recognize that sophisticated cyber intelligence tools like Pegasus can be misused to negatively impact individuals' right to privacy, chill free speech, and undermine public discourse. We take these risks seriously and work hard to eliminate or minimize, to the best of our ability, the likelihood of misuse of our products. As part of our human rights compliance program, we have taken concrete and specific steps, consistent with international standards, to address and mitigate human rights risks associated with our products. For example, we license Pegasus only to legitimate government agencies, specifically to serve national security and law enforcement objectives. We do not license our products to customers where, following our human rights-focused due diligence process, we believe there are inadequate protections in

place to mitigate the risk of misuse, or where country-specific conditions create an unduly high risk of misuse. We limit the number of instances in which our products can be used, and contractually require our customers to respect human rights and use our products only for legitimate intelligence and law enforcement purposes. Where a customer is accused of misusing our product, we investigate immediately. Where we believe a misuse has indeed occurred, we do not hesitate to take immediate action, which has included termination of a customer's right to use our product.

Since the establishment of our human rights compliance program in 2019, we have learned from our past experiences and continuously improved our processes. These include enhancements to our due diligence process, contractual safeguards, training and education, internal investigations, product design, and more.

What we do is important. How we do it is just as important.

Policies and Procedures

NSO Group's commitment to respect human rights and conduct our business responsibly is expressed in our policies and operationalized through related procedures. In September 2019, we adopted our Human Rights Policy, with full endorsement from our senior management and the Board of Directors. The Human Rights Policy is binding on all NSO Group employees and sets out the company's expectations of our business partners and customers. Since its adoption, the Human Rights Policy has been the foundation for our activities and the lodestar for our employees in fulfilling our commitment to respect human rights throughout our business activities. The key aspects of our Human Rights Policy include:

- A thorough evaluation throughout our sales process of the potential for adverse human rights impacts if a proposed customer were to misuse our products, including through examination of the past human rights performance, governance standards, and domestic legal frameworks of the country involved;
- Contractual obligations requiring our customers to limit the use of our products to the prevention and investigation of terrorism and serious crimes, and to only use our products in a manner that will not violate human rights under applicable laws and international norms;
- Specific attention to protect vulnerable individuals or groups at elevated levels of risk of arbitrary digital surveillance and communication interception;
- Periodic review of our human rights compliance program by compliance experts, coupled with a commitment to ongoing dialogue with stakeholders; and
- Cooperation with States in conducting their own investigations into alleged misuse of our products, along with fulfilling their duties to ensure that when product misuse occurs within their territories, those affected have access to effective remedies.

"[A]s responsible corporate citizens, we have committed ourselves to high ethical business standards, seeking to ensure that only vetted and legitimate government agencies will use our products and that we take all reasonable steps to prevent and mitigate the risks of adverse impact on human rights from their misuse."

As discussed in greater detail below, our Human Rights Policy is supported by the company's Human Rights Due Diligence Procedure, Internal Whistleblowing Policy, External Whistleblowing Policy, and Potential Product Misuse Investigations Procedure to form a comprehensive human rights compliance program.

We integrate our Human Rights Policy into our business processes in order to identify, prevent, and mitigate the risks of adverse human rights impact.

In October 2021, we adopted a new Code of Ethics and Conduct to complement the Human Rights Policy and further clarify the company's business and ethics standards for all our employees, contractors, officers, and directors, as well as business partners and customers. In addition to human rights, the Code of Ethics and Conduct encourages our employees to report any concerns, and describes our commitment to preventing bribery, corruption, and conflicts of interest, commitment to responsible procurement, compliance with export controls and sanctions, personal data protection, environmental responsibility, and equal opportunity and inclusion. The Code of Ethics and Conduct, together with the company's Human Rights Policy, Anti-Bribery and Corruption Policy, Third Parties Engagement Policy, Gifts and Hospitality Policy, Workplace Operation Policy, Sexual Harassment Prevention Policy, and Personal Data Protectionש Policy, codifies our holistic commitment to transparent and responsible business conduct.

Oversight and Governance

Consistent with the UNGPs, oversight of our human rights compliance program starts at the very top of our organization—with the Board of Directors, which has adopted the compliance policies and procedures discussed above, and regularly reviews business and human rights issues related to NSO Group's activities. The board appoints the members of the GRCC. The GRCC is comprised of NSO Group's CEO, Mr. Yaron Shohat, GC, Adv. Shmuel Sunray, one independent director, Dr. Yuval Karniel, a legal expert specializing in media policy and ethics and law in the media who also served as a board member of the Israel Broadcasting Authority and chaired its ethics committee and two additional directors, Mr. Omri Lavie and Adv. Anthony Levy.

The GRCC is empowered to approve, monitor, and review the company's governance, risk, and compliance policies, including those related to our human rights program. The GRCC also has final authority to approve or reject proposed sales identified as elevated-risk during our due diligence as being elevated-risk, including through the exercise of its right to veto a sales opportunity. Further, the GRCC may delay, reject, or approve a sale subject to additional safeguards or condition as it deems fit.

The GRCC has delegated responsibility for day-to-day implementation of NSO Group's human rights compliance program to the company's Management Committee, which consists of our CEO, SVP Business, and GC. The Management Committee meets at least once a month to discuss and review proposed business opportunities, any ongoing or pending internal investigations, engagement with stakeholders regarding human rights issues, and other items related to the company's human rights compliance program. The Management Committee is responsible and accountable for the company's decisions related to sales and reports its decisions to the GRCC at least every six months.

The Management Committee is closely supported by our Vice President for Compliance and Deputy General Counsel ("Deputy GC"), who has over 20 years of experience in corporate compliance and investigations with a particular emphasis on anti-corruption and human rights. The Deputy GC leads a dedicated team of three compliance attorneys ("Compliance Team"), who regularly interact with NSO Group's business and operational functions as well as relevant third parties to incorporate human rights considerations into the company's activities. These include ensuring that our new and existing products are evaluated from a human rights standpoint, vetting potential customers and renewing diligence on existing customers, developing and reviewing contractual safeguards, monitoring whistleblower hotlines and other public sources for any allegations of potential product misuse, conducting internal investigations, providing human rights-related training, monitoring the effectiveness of our processes, and seeking ways to further improve the overall human rights compliance program. The Compliance Team also collaborates with NSO Group's Legal Team to structure end-user agreements and ensure that human rights-related provisions are included to help mitigate potential adverse human rights impacts associated with the use of our products.

> After an extensive six-months collaborative investigation across multi organizations, we are thrilled to report the successful apprehension and dismantling a large, long-operating drug trafficking organization. Pegasus played a crucial role in this operation, providing invaluable real-time intelligence that facilitated accurate arrests of the organization's top leadership. Please share this with your team, expressing our appreciation for their hard work, as it played a crucial role in making this possible (*Western European client, August 2023*)

In addition, as mentioned in NSO Group's 2021 Transparency and Responsibility Report,[4] our Compliance Team works with leading external advisors and practitioners with a diverse set of capabilities and experience to evaluate the potential adverse human rights impacts of NSO Group's long-term strategies, targets, and goals. Our external advisors provide background reports regarding potential customers and their countries, including with respect to each country's human rights records, foreign relations, and domestic legal frameworks governing the use of cyber intelligence technology. The external advisors also provide ongoing assistance with various compliance-related work streams. Overall, our Compliance Team is responsible for implementing and championing a corporate culture that embraces respect for human rights, transparency, and responsibility, and working with our customers to improve their understanding of and adherence to NSO Group's human rights-related requirements.

Our Compliance Team plays a pivotal role in incorporating our human rights commitments into our business processes and cultivating a culture of compliance.

Assessment of Risks

NSO Group regularly assesses and reassesses the potential risks related to the use of our products. Through the ongoing human rights-focused analysis of our products, lessons gleaned from past investigations into allegations of potential product misuse, discussions with customers and other relevant stakeholders, and review of third-party reports, we have identified a number of salient human rights risks associated with our products and the wider cyber intelligence technology industry. Based on our observations, our most salient human rights risks include:

- The risk of potential misuse of our products against individuals and groups that act to protect or promote human rights in a peaceful manner, including but not limited to human rights defenders, members of civil society organizations, journalists, political activists, and lawyers;
- The risk of potential misuse of our products for reasons unrelated to national security or law enforcement;
- The risk of potential use of our products by unauthorized or untrained government agencies personnel, which is at odds with our contractual requirements and increases the risk of product misuse;
- The risk of potential use of our products in a manner inconsistent with domestic law and international human rights norms, such as in the absence of judicial or other independent approval processes and/or without adequate documentation of the reasons for requesting to conduct surveillance; and
- The risk of potential use of our products in countries where domestic regulations governing surveillance activities lack: (i) a defined scope of offenses that may warrant surveillance; (ii) a limit on the duration of surveillance activities; and (iii) a clear procedure to be followed when examining, using, sharing, or destroying information obtained through surveillance.

[4] NSO Group, Transparency and Responsibility Report 2021, pp. 13-14 (2021), https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf.

These risks, when realized, can result in violations of fundamental human rights, including:

- The right to privacy under UDHR Article 12 and ICCPR Article 17;
- The right to freedom of expression under UDHR Article 19 and ICCPR Article 19; and
- The right to freedom of assembly under UDHR Article 20 and ICCPR Article 21.

Moreover, there are a wide variety of additional risks that could arise in connection with our customers' use of our products. These include rights associated with the legal and judicial process, such as freedom from arbitrary arrest and detention (UDHR Articles 3 and 9, ICCPR Article 9) or improprieties in the legal process (UDHR Article 10; ICCPR Article 14), as well as invasions of freedom of thought, conscience, and religion (UDHR Article 18, ICCPR Article 18), restrictions on freedom of movement (UDHR Article 13, ICCPR Article 12), or participation in civic life (UDHR Article 21).

As outlined in the following sections, we have implemented our Human Rights Policy and accompanying procedures to help address and mitigate these salient risks. For example, we place great primacy on the customer due diligence review process and inclusion of strong contractual provisions. We are, however, aware that even the most rigorous due diligence and contractual measures are no guarantee that our customers will use our products responsibly and in a manner consistent with international human rights norms in every instance. This may be further compounded by our limited ability to monitor real-time use of our products by government agencies. Nevertheless, we continue to address these challenges through screening out customers in countries where the rule of law is weak, local laws do not meet international standards, or customer processes governing the use of our products provide insufficient assurances. Our approach is consistent with the approach taken in similar fields where the manufacturer or developer has limited visibility into how a customer might use its product, such as the defense industry.

Human Rights Due Diligence

We first adopted our Human Rights Due Diligence Procedure ("HRDD Procedure") in April 2020 to implement the Human Rights Policy and help the company comply with applicable local laws as well as international human rights standards. The multi-step HRDD Procedure requires the assessment of the potential human rights impact of a proposed business opportunity prior to the sale of our product to a customer, paying particular attention to the state of rule of law, human rights, and processes and institutional norms in the customer's country.

Consistent with the HRDD Procedure, we perform extensive due diligence on potential business opportunities. The HRDD Procedure consists of six major components: (i) initial risk assessment and classification; (ii) due diligence; (iii) final risk classification; (iv) review and approval; (v) mitigation; and (vi) renewal. These steps are designed to help identify, prevent, and mitigate the risks of adverse human rights impacts associated with potential misuse of our products.

Key Participants in Our HRDD Process

- **Compliance Team**, led by the VP for Compliance, sets the initial risk level for due diligence and administers the steps required under the company's HRDD Procedure.
- **General Counsel** provides the final risk classification for each proposed opportunity and participates on the Management Committee.
- **Business Units**, including our Sales, Client Executive, and Technical Support Teams, identify potential customers, gather relevant information to facilitate due diligence, help implement mitigation measures, and monitor post-sales activities.
- **Management Committee** reviews the results of human rights due diligence and determines whether to pursue a proposed opportunity and/or implement compliance recommendations, including any mitigation measures.
- **GRCC** retains the right to review and veto a proposed opportunity that has been deemed as elevated-risk.

Since 2021, we have rejected over USD 80M per annum for 3 years term in new business opportunities due to human rights concerns

This reflects roughly 35% of deal value sales applications that were submitted for consideration

From 2021 to date, approximately 10% of the potential new opportunities were rejected due to human rights concerns that could not be resolved or adequately mitigated.

Initial Risk Assessment and Classification

As part of the review required by the HRDD Procedure, when a new sales or marketing opportunity is identified, the business unit applies to pursue the new opportunity to the Compliance Team. Our Compliance Team then conducts an initial risk assessment to evaluate human rights-related risks associated with the proposed opportunity. The initial risk assessment is a two-part evaluation of the customer country and the nature of the proposed opportunity.

The country review incorporates nine external, widely recognized governance and human rights indices to evaluate the relative strength of the proposed customer country's protection of human rights. These sources provide insight into: (i) human rights and media freedom in the country; (ii) strength of the country's rule of law and political stability; and (iii) perception of corruption and transparency in the country. These sources include the World Bank Worldwide Governance Indicators, the Economist Democracy Index, Fund for Peace Fragile State Index, Freedom House Freedom in the World and Freedom of the Net reports, Reporters Without Borders Freedom of Press Index, Transparency International Corruption Perception Index, and Global Peace Index. In 2021, we added CIVICUS Civil Society Index and TRACE International Bribery Risk Matrix to further strengthen the baseline for our initial risk assessment and improve the overall human rights due diligence process.

Analyzing all of the above sources and using an internal scoring system that is reviewed annually and adjusted as necessary, the Compliance Team weighs relevant factors (e.g., human rights conditions including the level of freedom of expression, rule of law, political stability, perceived levels of corruption, and government effectiveness) to generate a "Country Score" between 1 and 100.

In addition to reviewing country-specific information, the Compliance Team evaluates risks related to each potential business opportunity and assigns an "Opportunity Category" of A, B, C, or D. In doing so, the Compliance Team considers, among other factors, the following: (i) product type to be sold; (ii) geographical boundaries within which the product could be issued; (iii) customer organization type and defined mission; (iv) duration of the proposed licensing agreement; (v) applicable export controls laws and regulations, including embargoes and sanctions; and (vi) customer's membership in international organizations and status related to major international treaties or conventions addressing human rights. To be clear, NSO Group does not sell any of our products to sanctioned countries, countries on the Financial Action Task Force (FATF) blacklist, or countries that do not pass our human rights due diligence.

	Opportunity Category			
Country Score	A	B	C	D
Above 60	Low	Low	Moderate	No Engagement
46–60	Low	Moderate	Elevated	
26–45	Moderate	Moderate	Elevated	
Below 25	No Engagement			

Based on the Country Score and Opportunity Category, the Compliance Team will classify the proposed business opportunity as: (i) low risk; (ii) moderate risk; (iii) elevated risk; or (iv) no engagement, as described in the above chart.

The company also maintains a list of 58 countries, referred to as "D countries", with which the company will not conduct business. This list undergoes an annual review and update by the Management Committee.

In 2021, NSO Group raised the threshold of the minimum Country Score required for client engagement from 20 to 25.

Due Diligence

Following the initial risk assessment and classification, the Compliance Team conducts a due diligence review. The steps required during this phase correspond to the proposed opportunity's assigned risk category and rely on information gathered from a number of sources, including open source research, discussions with NSO Group employees, interviews with potential customers, and background materials prepared by external consultants or investigative firms.

The information collected through these sources typically include: (i) denied parties checks; (ii) results of adverse media searches in English and relevant local languages; (iii) domestic legal framework governing surveillance activities and data protection; (iv) internal processes and safeguards in place at customer organization; (v) reputational information relevant to human rights; (vi) strategic input from interested government parties; and (vii) analyses of applicable export control laws as well as embargoed countries and specially designated nationals ("SDN") lists.

The following chart summarizes the due diligence requirements for each risk level:

	Risk/Source	Low	Moderate	Elevated
Open Source Intelligence	Results of open source adverse media search	✓		
	Report prepared by external investigative firm providing results of local language adverse media search, customer organization overview, and foreign policy and human rights-related information		Level 1	Level 2
Human Intelligence	Sales Manager questionnaire	✓	✓	✓
	Client Executive activity report [N/A for renewals]	✓	✓	✓
	Technical Support questionnaire [N/A for new End-User]		✓	✓
	Partner questionnaire	✓	✓	✓
	Advanced intelligence collected by external investigation firm		Level 1	Level 2
	Strategic input from government authorities			✓
Legal Framework	Publicly available information about local domestic legal framework		✓	
	Local legal opinion			✓
	Export controls (EU, United States, Israel)		Level 1	Level 2
	SDN / embargoed countries	Level 1	Level 2	Level 2
	End-user questionnaires/interviews			✓

Final Risk Classification

Once the Compliance Team completes the required due diligence steps outlined in the HRDD Procedure and prepares a memorandum summarizing the results and any proposed mitigation plans, the General Counsel reviews and determines the final risk classification. In other words, based on a review of the relevant materials, the General Counsel may confirm or adjust the Compliance Team's initial risk classification. If the General Counsel determines that it is necessary to adjust the risk classification to a higher risk category than the initial classification, then the Compliance Team is required to conduct additional due diligence activities as appropriate under the HRDD Procedure.

Review and Approval

Following the General Counsel's confirmation of the risk classification and completion of any additional due diligence steps, the request to pursue the proposed business opportunity is subjected to final review and approval. All proposed engagements must be reviewed by the Management Committee. In addition, the Management Committee provides a report describing all opportunities reviewed, including the outcome, to the GRCC every six months. The GRCC also has the authority to review all proposed engagements where, based on the results of human rights due diligence: (i) there is an elevated level of risk; (ii) the Management Committee's approval was not unanimous; (iii) in the reasoned opinion of the Management Committee the sale requires the GRCC's attention; or (iv) at the request of the GRCC.

Moderate- and elevated-risk opportunities are subjected to a wide array of mitigation measures to prevent or minimize the risk of product misuse.

Mitigation

For opportunities classified as moderate- or elevated-risk, we undertake some or all of the following measures to prevent or minimize the risk of product misuse:

- Enhanced human rights training and contractual safeguards for operators and management;
- Periodic customer certifications and declarations, including prior to maintenance renewals;
- Periodic on-site audit by the company's Compliance Team or by an independent third-party auditor;
- Monitoring of applicable public reports suggesting human rights violations, including instances that do not involve NSO Group products;
- Enhanced technological restrictions related to volume, number of installations, geographic coverage, and more;
- Periodic activity reports submitted by client executives;
- Periodic review of open source information focusing on human rights and surveillance in specific countries;
- Additional review by both internal and external sources;
- Contractual limitation on certain targets; and
- Additional specific mitigations to address the unique circumstances of each customer engagement, where appropriate.

Renewal

The HRDD Procedure further requires that the due diligence be renewed annually or sooner, if required as part of a mitigation plan or in case there are material changes to the customer relationship that would warrant such a review.

Due diligence is renewed annually or sooner if there are material changes to the customer relationship that would warrant such a review.

Regulatory Oversight

While we have undertaken substantial efforts to establish a comprehensive and robust internal framework to prevent misuse of our products, the sale of our products also is subject to an in-depth regulatory scrutiny. Following completion of our human rights-focused due diligence, our marketing and sales activities are subject to review by export control authorities in the countries from which we export our products: Israel, regarding Pegasus, and Bulgaria, regarding other tactical and network products. Specifically, Israel's DECA imposes its own constraints on the licensing of Pegasus. DECA performs an independent evaluation of potential customers, including from a human rights standpoint. In fact, in several instances, DECA has refused our applications for export licenses. In other cases, we terminated engagements with customers who already had valid export licenses after identifying new political, legal, diplomatic, or human rights risks through our ongoing diligence.

Contractual Requirements

We require, at a minimum, the inclusion of human rights compliance provisions in all our customer agreements, with additional human rights-related assurances inserted based on identified risks or mitigation plans. Our standard customer agreements include obligations to comply with all applicable laws and

regulations, including laws and regulations governing the use of our products and similar tools, as well as international human rights norms.

In general, our customers are required to:

- Fully and strictly comply with all applicable domestic laws and regulations, including but not limited to those related to surveillance activities, the rights to privacy and freedom of expression of individuals, and obligations to obtain judicial warrants, consents, approvals, and/or decrees to the extent required by law for each and every use of the company's product;

- Receive and review NSO Group's Human Rights Policy and understand the terms expressed therein;

- Use the company's product only for the legitimate and lawful prevention and investigation of terrorism and serious crimes as defined in the agreement;

- Respect human rights contained in the International Bill of Human Rights and in the International Covenant of Political and Civil Rights, including but not limited to the right to freedom of expression and the right for protection against unlawful and arbitrary violation of privacy, and fully and strictly adhere to human rights norms at all times in using the company's product;

- Not use the company's product to target individuals or groups because of their race, color, sex, language, religion, political or other opinions, national or social origin, property, birth or other status or their otherwise lawful exercise or defense of human rights;

- Not use the company's products against officials of any foreign governments;

- Establish and maintain a procedure for grievances by third parties through which such third parties can raise complaints regarding human rights-related concerns;

- Immediately notify NSO Group of any knowledge regarding a misuse or potential misuse of the company's product which may result in a violation of human rights;

- Investigate any allegations of human rights violations in connection with the use of the company's product and notify the company of the results of that investigation;

- Take appropriate remedial action where such investigations confirm that human rights violations have occurred, which may include deletion of data obtained, re-training or discipline of customer personnel responsible for misuse, or other measures designed to prevent the recurrence of misuse;

- Cooperate with the company with regards to any inquiry, dispute, or controversy, including through disclosure of relevant documents and interviews with key personnel;

Moreover, where not clearly defined under the customer's domestic law, where domestic law is not fully aligned with international norms, or where not otherwise set forth by applicable regulations, we contractually require our customers to:

- Formulate and strictly abide by a surveillance procedure or protocol for the use of the company's products. For example, such procedure or protocol must be consistent with international norms and include and/or specify: (i) legitimate surveillance request supported by evidence; (ii) suspected crimes; (iii) surveillance duration and renewals; (iv) data retention period; and (v) approval granted in writing by a duly authorized independent oversight authority in accordance with local laws.

- Include clauses defining specific crimes and terrorism-related activities in respect of which our products may be used to prevent or investigate.

We include human rights compliance clauses in all our customer contracts, with additional, enhanced assurances inserted based on identified risks.

Permissible Use

Terrorism is defined as unlawfully and intentionally causing, attempting, or threatening to cause: (i) death or bodily injury to any person; (ii) serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or the environment; or (c) damage to property, places, facilities, or systems, resulting or likely to result in major economic loss. This includes when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act. This also includes participating as an accomplice, organizing or directing others, or contributing to the commission of such offenses by a group of persons acting with a common purpose.

National Security Threats are defined as genuine threats against the existence of the nation or its territorial integrity or political independence by force or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government, and are not merely local threats or relatively isolated threats to law and order. National Security Threats do not include threats unrelated to national security, including, for example, the embarrassment of, or exposure of wrongdoing by, the government, or diminishing government's ability to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

Serious Crimes are defined as the crimes of trafficking of persons, illicit trafficking of arms, trafficking of narcotics, child pornography, crimes of violence, threats to children, financial crimes, and organized crimes/racketeering.

Training and Communication

We continue to implement and reinforce our Human Rights Policy through employee training and communication. For example, all new employees of NSO Group receive human rights training as part of their on-boarding process. In addition, we provide regular human rights training to our employees in key functions, including sales, marketing, technical support, and others involved in direct interactions with customers. Our Deputy GC also meets periodically with the company's R&D Team to ensure that each new and existing product is evaluated from a human rights standpoint.

Between January 2021 and December 2023, we held human rights training sessions for a total of 546 participants across all company's departments.

We also provide comprehensive human rights training to our customers as appropriate. This training includes a discussion of human rights obligations under international standards and norms, and customer responsibilities with respect to the use of our products. From 2021, approximately 14 customers attended human rights training sessions conducted by our Compliance and Training Teams.

In 2023, we developed a tailored ethics and compliance training program for our business partners to further ensure that NSO Group's commitments to uphold human rights and conduct business responsibly are understood and replicated by all those who work with us. This training includes an overview of our key compliance policies, including Human Rights Policy, and focused sessions on anti-bribery and anti-corruption compliance and human rights compliance.

We provide comprehensive human rights training to our employees, customers, and business partners to implement and reinforce the Human Rights Policy.

Ongoing Review

All customers are subject to ongoing oversight for compliance with the terms of their agreements and our Human Rights Policy. Because we do not have real-time insight into the use of our products, there are significant challenges in ensuring effective monitoring. For instance, intelligence and law enforcement agencies operate with strict confidentiality requirements, including where required by local laws and regulations, and are explicitly prohibited from or are extremely reluctant to share information with a private company to prevent inadvertently compromising sensitive information related to national security or the

investigation of serious crimes. Despite these challenges, we regularly engage with our customers to discuss NSO Group's human rights requirements and related expectations for customer operation of our products. We also constantly monitor public reporting by the media and civil society organizations that may suggest potential misuse, and are always seeking additional ways to improve our oversight approach.

Reporting and Investigation

Consistent with the UNGPs, we encourage both internal and external stakeholders to raise concerns of misconduct with us. Our grievance mechanisms, codified in the company's Internal Whistleblowing Policy and External Whistleblowing Policy, allow both confidential and anonymous reporting.

The Internal Whistleblowing Policy, adopted in September 2019, emphasizes our "open door" approach and support for whistleblowers who raise concerns in good faith, and provides protection from retaliation. This policy applies to all NSO Group employees, consultants, officers, and directors, and specifies channels through which they can escalate concerns to the company's most senior management. Internal whistleblowers can, for example, raise concerns with their immediate supervisors, communicate directly to NSO Group's CEO, GC, or Deputy GC, Or send an email to our confidential whistleblowing account. Though anonymous reporting is supported, interaction with investigators is encouraged , as doing so allows for a more thorough collection and review of all key facts.

Since 2021, we have opened 19 investigations into allegations of potential product misuse.

The External Whistleblowing Policy, also adopted in September 2019, encourages external stakeholders, including business partners, customers, and potentially affected individuals, to report a grievance related to NSO Group's products and/or services through a confidential email account, which is regularly monitored and reviewed by our VP for Compliance. This policy also encourages interaction with investigators but assures protection against retaliation. In the past, where a whistleblower preferred not to communicate directly with NSO Group, we arranged communications through a mutually agreed third party, who maintained the whistleblower's confidentiality, to further discuss and address the whistleblower's concerns.

In addition to maintaining formal grievance mechanisms, we closely monitor and track public reports as part of our ongoing efforts to identify and investigate, where possible and appropriate, any instances of potential product misuse. Recently, the vast majority of allegations of potential product misuse have come from external sources, including media reports and statements from civil society organizations and human rights groups. Between January 2021 and present, we received 39 reports through our external whistleblowing channels and through media and civil society outreach. All reports were examined, reviewed and addressed by NSO Group's Compliance Team. Many of the reports were found baseless and no additional remedial actions were needed. The reports ultimately led to the termination of engagement with 6 customers due to investigative findings of possibility of systematic product misuse. These statistics reflect a significant reduction in product misuse reports compared to previous years. This positive trend can be attributed to the diligent efforts and effectiveness of our human rights compliance program.

We encourage both internal and external stakeholders to raise concerns related to our products and/or services at any time without fear of retaliation.

Once we receive a report from a whistleblower or otherwise identify a concern, including through public reports, we review and investigate in accordance with our Potential Product Misuse Investigations Procedure. This procedure, adopted in April 2020, aims to ensure that each investigation is conducted consistent with a number of investigative goals, including to:

- Comply with applicable laws and NSO Group policies, including the Human Rights Policy;
- Respect the rights of all stakeholders;
- Determine key facts and causes;
- Perform investigations objectively and expeditiously;
- Draw appropriate conclusions, balancing the rights of stakeholders;
- Undertake appropriate remedial action, if applicable; and
- Preserve confidentiality of the incident reporter to avoid or minimize retaliation, if applicable.

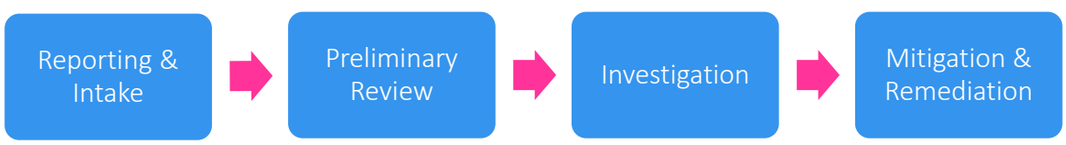
For all credible allegations of potential product misuse, we conduct a thorough preliminary review to determine whether a full investigation should be opened.

In all cases of credible allegations of potential product misuse, our Compliance Team conducts a preliminary review to determine whether there is sufficient information and technical basis to appropriately investigate the allegation. This preliminary review, while driven by the specific circumstances of individual cases, typically consists of identifying key alleged factual details, such as identities of potential end-user organizations, circumstances that have led individuals to believe they were targeted using our product, and alleged dates and locations of product installation. Based on the analysis of the available information, the Compliance Team works with the business to determine the technical feasibility of the alleged conduct. For example, we try to ascertain whether an alleged end-user organization is indeed our customer, and if so, whether that particular customer had access to use the product in question at the time the alleged conduct reportedly occurred.

Following the preliminary review, the Compliance Team presents the initial findings and recommendations to the Management Committee, which then determines whether to proceed with a full investigation and, if so, appoints an investigation team led by an attorney. Investigations may include a review of further data, interviews, meetings, and an evaluation of objective risk factors, including an analysis of whether the customer has engaged in previous publicly-reported human rights abuses. The investigation team will seek to obtain and evaluate information from the customer, such as details about the process followed in connection with the use of our product to target the specific individuals. As discussed above, our customers are contractually required to cooperate with our investigations and provide relevant information. Refusal to cooperate can result in the suspension of the customer's right to use our product until further notice.

Indeed, the investigation team pays particular attention to whether and how the customer adhered to the domestic legal framework and protections, surveillance request and approval processes, and international human rights norms. This analysis includes a review of the legal basis for the customer's use of NSO Group's product, their interference with individual human rights at issue,

and whether the customer applied sufficient safeguards when obtaining intelligence using our product. Where appropriate, we may seek further input from external experts, such as local counsel with relevant experience.



Investigation results are shared with the Management Committee and the GRCC to collaboratively determine next steps and potential remediation. Depending on the outcome of the investigation, when warranted, NSO Group takes appropriate corrective action ranging from re-training to termination of the customer relationship. In some cases, we are unable to conclusively determine whether there was—or was not—a misuse of our products. In those instances, we develop and implement additional mitigation measures designed to prevent future misuse.

In the last two years, we have suspended or terminated the accounts of 6 customers as a result of those investigations, resulting in 57 million USD in revenue loss.

Through our experience conducting these investigations, and with recommendations from our external advisors, we have strengthened our initial due diligence and review processes, contractual provisions, and human rights training for customer personnel. Nevertheless, a number of inherent challenges remain given the distinct missions of our customers and the nature of their intelligence and law enforcement operations. For instance, because of our customers' confidentiality requirements, we are unable to provide actual or alleged victims with information about adverse impacts or implemented remediation, or even acknowledge or deny the existence of relationships with specific customers. We cooperate with governments to try to ensure that when abuses occur within their jurisdictions, those affected have access to effective remedy, but the confidentiality restrictions limit our ability to do much more.

At a minimum, we contractually require our customers to establish a grievance procedure, investigate any allegations of product misuse, and take appropriate remedial action when such investigations confirm that human rights violations have occurred—all in addition to cooperating with NSO Group's investigations into potential product misuse. Nevertheless, there are obvious and serious limits as to how much a private company can require of a sovereign government entity or enforce those contractual requirements against such an entity. While we follow the approaches described in the UNGPs to the best of our ability with respect to remediation, both the UNGPs and we, ourselves, recognize that this is a complex and difficult area in particular for our sector.

Where we identify product misuse, we take immediate and decisive action, including termination of customer's right to use our product.

Technological Safeguards

NSO Group is proud to be the first company in the cyber intelligence technology sector to publicly commit to respect human rights in line with the UNGPs and other international human rights standards. Over the course of 2022 and 2023, we have redoubled our efforts to continuously enhance our human rights compliance program and mitigate risks. As part of this ongoing effort, we are reviewing product design options to incorporate stronger, technologically enabled human rights safeguards.

We have already engineered a number of human rights safeguards into our products. For instance, we tailor the configuration of the Pegasus system with specific settings for each end-user in accordance with the limitations outlined in their contracts as well as export licenses issued by the Israeli DECA. This allows us to restrict the scope of the Pegasus system's capabilities and customize the terms of use for every customer. Such configurations cannot be bypassed, changed, or altered by customers, as these are located in a secure part of the system that customers are not authorized to access. In other words, only NSO Group has the ability to manage the technological configuration of Pegasus, and the system cannot be used by anyone other than customers who have been vetted through our human rights due diligence process.

We are continuously reviewing product design options to incorporate stronger, technologically enabled human rights safeguards.

We have also developed and implemented a "kill switch," which allows NSO Group to remotely and unilaterally shut down the Pegasus system to prevent the end-user from operating the system. In the event we use the kill switch, the entire Pegasus system is deactivated and automatically disconnected from the devices on which it was installed, and the customer can no longer monitor new or existing targets. It is technically impossible for the customer to reverse our shut-down or to restart the system following such shut-down. As a result, the customer will not be able to use the system again unless we take further action to allow re-access to the system.

The Pegasus system's audit log constitutes another important tool in investigating potential misuse by end-users. In the course of an investigation and with the customer's permission, the activities of each operator can be audited, including the target device identifiers. The audit log remains immutable and cannot be bypassed, altered, or deleted by the customer or an operator.

Moreover, to strengthen the target verification process, the Pegasus system now requires an extra validation step to check the target device identifier against a predefined "blocklist" and initiates an automatic uninstallation if the target device identifier is on this list. In addition, we have instituted an email address verification protocol designed to prevent the use of Pegasus to target certain government officials, military personnel, or employees of an affiliate organization.

> "Your tools were actively used to support our efforts during the kidnapping of one of our citizens. We had no possibility of intervening without harming the hostages. With Pegasus, we managed to gain access to the kidnappers' devices to extract the necessary information, enabling us to find the right moment to intervene and free the hostages (Western European client, September 2023)."

We have also incorporated an "operator statement" into our technological platform, which requires operators to affirm the legality of the installation. The operator statement requires the operators to provide specific information for each installation request, including details about the authorization to target the device, any supporting documents, the relevant legal provision associated with the suspected misconduct, and the name of the approving authority. This mechanism was added to our already existing "warrant management system" option, which was also expanded to support different kinds of warrants with limitations and restrictions tailored to each specific type of warrant or court order. These features were specifically designed to aid intelligence and law enforcement agencies utilizing our technology in strict adherence to their respective domestic laws and regulations. We are in the process of formulating the operator statement and warrant management system requirements for certain types of customers.

Stakeholder Engagement

While we have undertaken and continue to undertake appropriate steps to mitigate risks of misuse of our products, there are obvious limits as to what a single private company can do to monitor the actions of customers, particularly when those customers are duly authorized intelligence and law enforcement agencies of sovereign governments engaged in highly sensitive and confidential investigations. We strongly believe that global standards must be developed to assist in guiding our industry as a whole. To try to turn those beliefs into actions, we have engaged and sought to engage with numerous stakeholders ranging from government entities, parliamentary or congressional committees, international organizations, civil society organizations, professional associations, and academics. We hope that our readiness and willingness to engage and seek feedback is reciprocated to improve mutual understanding of the risks and challenges associated with balancing the state duty to protect the physical security of its citizens with the potential misuse of cyber intelligence technology against political dissidents, journalists, human rights activists and other vulnerable populations.

Similarly, while we are committed to transparency and continue to be one of the most forthcoming companies in the cyber intelligence technology sector, we are under strict regulatory and confidentiality restraints that significantly limit our ability to share customer information publicly. Continuing dialogue, including multi-stakeholder exchanges and multilateral efforts that encompass governments, industry representatives, academic communities, and civil society, therefore remains key to appropriately regulating this sector and protecting all rights of individuals.

We are committed to transparency and continue to be one of the most forthcoming companies in the cyber intelligence technology sector.

Highlights from 2022–2023

Throughout 2022 and 2023, we have undertaken a number of actions to further strengthen our protection and promotion of human rights, increase transparency, and champion the development of a robust regulatory framework to ensure effective and responsible use of cyber intelligence technology.

Studying Impact on Journalists

In light of certain allegations regarding potential misuse of our products against journalists and other members of the media, and as part of an ongoing effort to address potential human rights impacts associated with the use of our products, we have been studying the scope and nature of potential impacts of our products on journalists and the press. Last year, we began researching and collecting publicly available data points on reported instances of potential misuse of Pegasus against journalists. We focused on identifying and evaluating patterns of potential impacts associated with allegations of misuse of our products against journalists, which did not entail an assessment of the merit or credibility of such allegations.

Based on the available data points, we started analyzing key information about the alleged targets, including their country of residence, demographic information, journalistic reporting activities, and any reported prior interactions with government authorities. To date, we have identified several preliminary trends with respect to these allegations. We have incorporated these initial observations into our human rights due diligence process and are continuing to evaluate the potential impacts of our products on journalists in order to develop more tailored mitigation strategies.

Heightened Due Diligence and Oversight

Over the past several years, we have sought to continuously improve NSO Group's human rights compliance program, including the human rights due diligence process. In relation to that initiative, our Compliance Team has progressively and significantly increased the company's engagement with potential customers as part of the due diligence review process. For example, our VP for Compliance has conducted more frequent in-person interviews and site visits to customer locations to obtain a more complete understanding of customer organizations and processes, and provide enhanced guidance on NSO Group's human rights-related requirements. Where a customer is onboarded following due diligence review, this level of engagement continues over the duration of the relationship, allowing us to periodically check on the customer's understanding of our human rights requirements, provide tailored human rights training and education to customer personnel, and better evaluate the customer's commitment to human rights.

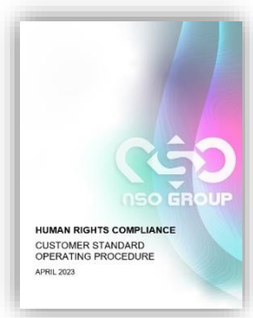
Since 2022, compliance related expenses accounts for over 10% of the total General and Administrative (G&A) expenditures

Enhanced Guidance for Customers

To further mitigate the risk of misuse of our products, we developed a detailed Standard Operating Procedure ("SOP") for customers where, following a due diligence review, we determined that there is an elevated risk that the customer's existing processes for evaluating the appropriateness of monitoring a particular target using our product may not be fully consistent with international norms.

This SOP, developed in consultation with our external business and human rights advisors, specifically instructs end-users to consider whether a target is a human rights defender, a journalist,

a lawyer, or a political dissident, and if so, to exercise heightened care. Another key aspect of the SOP is that it requires end-users to create an "auditable record" that NSO Group—or a mutually agreed independent third party—can access with customer consent and review if allegations of product misuse subsequently arise. The SOP is designed to help our customers operate our products in accordance with established international human rights standards and our contractual requirements, including by following internal processes that address substantive and procedural considerations, and also to generate accountability within our clients.



In accordance with NSO Group's Human Rights Policy and accompanying procedures, this Human Rights Compliance Standard Operating Procedure sets forth the compliance expectations and requirements to which NSO Group's customer must adhere in the course of obtaining, operating, or purchasing licenses for NSO Group products. NSO Group requires that customer strictly abide by the requirements and the protocol set forth in this SOP, and independently manage and ensure the implementation and enforcement of this SOP.

Cooperation with International Authorities

At NSO Group, we are committed to transparency and corporate responsibility. We have cooperated with inquiries from external stakeholders, including state authorities. For example, on June 21, 2022, NSO Group's Deputy GC participated in a hearing organized by the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware ("PEGA Committee"). During the PEGA Committee hearing, our Deputy GC provided the European lawmakers with further insight on NSO Group's Pegasus technology, the core principles that guide the manner in which it has been developed and licensed, and the inherent challenges that companies like NSO Group face in implementing and enforcing human rights safeguards. Our Deputy GC also provided a comprehensive overview of our human rights compliance program and called for a global regulatory framework. Following the hearing, NSO Group has hosted members of the PEGA Committee at our headquarters in Israel.

This past year, NSO Group hosted members of the of the UN Working Group on Business and Human Rights at our offices in Luxembourg to provide context about (i) the operations of private companies in the cyber intelligence technology sector, (ii) NSO Group's efforts to balance the responsibilities of our government customers to protect their citizens from harm and our own responsibilities to reduce the likelihood of misuse of our products, and (iii) NSO Group's readiness to engage in meaningful discussions.

NSO Group remains committed to answering questions and replying to inquiries from regulators and broader stakeholders, and welcomes opportunities to offer our perspective on complex questions surrounding the use of cyber intelligence technology.

Over the past several years, we have sought to continuously improve our human rights compliance program, including the human rights due diligence process.

Engagement with Civil Society and Other Stakeholders

NSO Group has, and continues to explore new opportunities to, actively engage with various human rights groups and contribute our hard-learned expertise to discussions about global best practices. NSO Group continues to investigate and respond to allegations of product misuse raised by NGOs, civil society organizations, and media outlets.

In addition, NSO Group's GC and Deputy GC actively contribute to academic and broader public dialogue by participating in various forums and lecturing on pertinent subjects. Notably, our GC and Deputy GC each serve as guest speakers in courses related to international law, human rights law, anti-corruption compliance, export controls and counter terrorism, in various prestigious universities, colleges and in other continuing education programs. Our GC's commitment includes being a permanent lecturer in the course for advance certification in regulatory compliance, a collaborative initiative organized by the International Compliance Association, the Israeli Bar Association and the Israeli Association for Compliance & Administrative Enforcement.

Our GC and Deputy GC also respond to media inquiries and contribute to industry best practices by sharing information about compliance issues and NSO Group's practices with other defense companies. In addition, our Deputy GC, for example, was a recent guest in the "Bribe, Swindle or Steal" podcast, a leading financial crime podcast.

Supporting International Standards

We have long called for and continue to support the establishment of an international framework for regulating the development, sale, and use of cyber intelligence technology. Without an international framework, regulation is effectively left to fragmented and uncoordinated national legislative efforts. Disparate national legislation may unintentionally create incentives for countries to have weak regulatory frameworks for either their own information gathering or propaganda purposes or as an incentive to develop a cyber surveillance industry within their borders. An international framework would bring more clarity, precision, transparency and legal certainty to all actors, including companies, customers, civil society, and regulatory authorities. In particular, an international framework should address and define what constitutes legitimate use versus illegitimate use of cyber intelligence technology. As such, we welcomed the recent position paper published by the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, titled Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, although we believe that the framework called for therein must go further and address the end-users of cyber intelligence technology, as outlined in Article 20 of the United Nations Convention on Organized Crime.

Indeed, while private companies must act responsibly in developing and selling cyber intelligence solutions, governments, as end-users of the technology, have the ultimate obligation—and the control—to ensure that their intelligence and law enforcement agencies deploy the technology as intended for legitimate prevention and investigation of terrorism and serious crimes. Private companies have limited ability to influence government customers' decisions, or to enforce contractual requirements or international norms against state entities. Thus, to be effective, an international framework must consider both the states' duty to ensure public safety and respect human rights as well as the responsibilities of private companies.

Specifically, we believe that an international framework governing the development, sale, and use of cyber intelligence technology should:

- Recognize the need to balance protecting the rights of those targeted with cyber intelligence tools, including the rights to privacy, freedom of expression, and freedom of assembly, with the need for legitimate uses of this technology when legally warranted to address criminal and national security concerns and thereby protect citizens' fundamental rights to life and security;

- Be built through a global multi-stakeholder approach, including through dialogue and collaboration across civil society organizations, national and international governments and agencies, the private sector, and the companies developing these tools;

- Make the acquisition of cyber intelligence tools subject to robust public oversight, consultation, and control, in order to comply with safeguards against illegitimate access or use, and to guarantee the principles of necessity, proportionality, legality, legitimacy, and due process;

- Address and define what constitutes legitimate use versus illegitimate use of cyber intelligence technology;

- Establish ground rules regarding transparency for companies and states, as well as guidance on corporate best practices for companies developing cyber intelligence technology to mitigate risks of potential product misuse;

- Address the need for an independent and objective international body to conduct investigations on misuse of cyber intelligence technology;

- Establish ground rules regarding the provision of remedies when appropriate; and

- Provide safeguards for companies that develop and provide cyber intelligence technology consistent with the requirements of such an international framework.

During 2022 and so far in 2023, we have engaged with various stakeholders—including national lawmakers and regulators, international organizations, academics, and civil society organizations—regarding the need for a robust international regulatory framework. We continue to stand ready to engage constructively in this process and welcome any opportunity to collaborate with stakeholders.

Looking Ahead

Moving forward, as we strive to further strengthen our human rights compliance program and related initiatives, we plan to deepen our activities in a number of areas, including:

- Continuing to consider the impact of our products on certain vulnerable populations, including journalists, human rights defenders, and political dissidents, and plan to proactively engage with representatives of vulnerable communities to understand their concern and avoid negative impact on their rights;

- Continuing to seek opportunities to meaningfully contribute to the development of an international framework for regulating the development, sale, and use of cyber intelligence technology;

- Developing and implementing additional technological safeguards that can help to identify and mitigate the likelihood of product misuse, such as system-based solutions to block any attempts to target the phone numbers of registered journalists;

- Measuring and evaluating the effectiveness of our human rights-related processes and programmatic activities through a focused compliance audit;

- Continuing to use our best efforts to ensure that our customers use our technology responsibly and legally, avoiding any actions that might infringe upon human rights;

- Promoting improved access to effective remedies for victims of misuse of our products, including by increasing relevant requirements in contract terms and pursuing legal action against customers responsible for product misuse and adverse human rights impacts;

- Further developing approaches to increase transparency, despite our inherent constraints;

- Increasing the amount of ongoing human rights training provided by NSO to clients' operators to improve awareness of operator responsibilities; and

- Further develop processes to safeguard human rights.

We believe these activities will help us improve our existing processes, identify and add new and better ways to protect human rights, and continue to serve as an industry leader to inspire other companies in our sector to adopt similar measures.