Conducting our business with integrity

Our business is built on the foundation of trust. Our Code of Conduct expresses our personal commitment to earn this trust every day, in all of our business activities and in every country where we work. It reflects our values through clear and simple direction for all of our employees and business partners and defines the principles of ethical and compliant business practices.
Highlights in 2018

- **887** Ethical concerns reported through our Ethics Helpline
- **364** Sustainability audits implemented in supply chain
- **210** Ombuds leaders in 75 countries in more than 150 cities
- **One of the World’s Most Ethical Companies** as honored by the Ethisphere Institute in 2018 and 2019

**Internal Human Rights**
Impact Assessment undertaken by external assessor
Ethical and responsible business

Integrity is at the core of how we do business and our Code of Conduct provides the foundation for our employees and other stakeholders to act responsibly.
### Our commitments, targets, and performance

#### Priority area

<table>
<thead>
<tr>
<th>Conducting business with integrity</th>
</tr>
</thead>
</table>

#### Material topic

<table>
<thead>
<tr>
<th>Ethical Business Practices and Corporate Governance</th>
</tr>
</thead>
</table>

#### Targets

<table>
<thead>
<tr>
<th>Priority area</th>
<th>Material topic</th>
<th>Targets</th>
<th>Achievements 2018</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conducting business</td>
<td>Ethical Business Practices and Corporate Governance</td>
<td>2020</td>
<td>Employee/Line Manager engagement on importance of ethics and compliance. 75% favorable answers targeted.</td>
<td>Progress of this target is measured with a question in our anonymous employee survey (CCT) “Does your line manager periodically talk with you and your team members about the importance of ethics and compliance?” In 2018 77% (72% in 2017) of responding employees gave a favorable response.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2030</td>
<td>Employee/Line Manager engagement on importance of ethics and compliance. 85% favorable answers targeted.</td>
<td>Ongoing – on track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2018</td>
<td>Ethical Business Training (EBT) completion: 95%.</td>
<td>The training was completed by 95% of Nokia employees. Assured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2020</td>
<td>EBT completion: 98%.</td>
<td>Ongoing - not on track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2030</td>
<td>EBT completion: 100%.</td>
<td>Ongoing - not on track</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NEW target 2020 (to replace the 2020 and 2030 targets): Ethical Business Training (EBT) completion: 95%.</td>
<td></td>
</tr>
</tbody>
</table>
## Our commitments, targets, and performance

<table>
<thead>
<tr>
<th>Priority area</th>
<th>Material topic</th>
<th>Targets</th>
<th>Achievements 2018</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conducting business with integrity</td>
<td>Privacy and Data Security</td>
<td><strong>2020</strong>&lt;br&gt;Our aim for 2020 is that Nokia be recognized as an industry leader in security and privacy. This will be assessed through external benchmarking.</td>
<td>Protection of critical information ecosystems on target level, 95% of identified critical and high audit findings closed. Employee engagement with security culture program clearly above targets.</td>
<td>Ongoing - on track</td>
</tr>
<tr>
<td></td>
<td><strong>2019</strong>&lt;br&gt;Successful completion of the first GNI assessment.</td>
<td></td>
<td>Preparation for the GNI assessment was started in late 2018 and will be completed by October 2019.</td>
<td>Ongoing - on track</td>
</tr>
<tr>
<td></td>
<td><strong>2020</strong>&lt;br&gt;Nokia as externally recognized leader in vendor related issues in freedom of expression and right to privacy according to external benchmarking, e.g. Ranking Digital Rights.</td>
<td></td>
<td>In 2018 we continued our strong Human Rights Due Diligence (HRDD) program to mitigate potential misuse of technology to limit freedom of expression and privacy. We published further anonymized cases in this report and continued to engage in stakeholder dialog through speaking and other events.</td>
<td>Ongoing - on track</td>
</tr>
</tbody>
</table>
## Our commitments, targets, and performance

<table>
<thead>
<tr>
<th>Priority area</th>
<th>Material topic</th>
<th>Targets</th>
<th>Achievements 2018</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conducting business with integrity</td>
<td>Labor conditions / suppliers and partners</td>
<td><strong>2020</strong></td>
<td>Comprehensive supplier sustainability risk mitigation (90% of suppliers assessed with Satisfactory Sustainability Score and 100 on-site audits conducted per year).</td>
<td>Assured</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>2020</strong></td>
<td>74% suppliers achieved a satisfactory EcoVadis score (71% in 2017) and we conducted 75 on-site audits (72 in 2017).</td>
<td>Ongoing – not on track</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>2020</strong></td>
<td>Establish supplier worker empowerment program (enabling trainings on NokiaEDU and Worker Tollfree Helpline).</td>
<td>Assured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Nokia Ethics Helpline enables capturing supplier grievance. Channel is communicated to suppliers at Suppliers Corporate Responsibility Workshops.</td>
<td>Ongoing – on track</td>
</tr>
<tr>
<td></td>
<td>Materials traceability and conflict minerals</td>
<td><strong>2018</strong></td>
<td>Achieve full traceability to the smelters in our supply chain and their conflict-free status (Mobile Networks).</td>
<td>Assured</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>2020</strong></td>
<td>97% of our suppliers have achieved full visibility into the smelters in our supply chain.</td>
<td>Not achieved</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>2020</strong></td>
<td>84% of smelters identified as part of Nokia's supply chain were validated as conflict-free or are active in the validation process.</td>
<td>Assured</td>
</tr>
</tbody>
</table>

(The same percentages are valid both for Mobile Networks and Nokia Group.)
## Our commitments, targets, and performance

### Priority area

<table>
<thead>
<tr>
<th>Material topic</th>
<th>Targets</th>
<th>Achievements 2018</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Conducting business</strong></td>
<td><strong>Health, Safety, and Wellbeing</strong></td>
<td>100% of all suppliers delivering high-risk activity to be assessed using Nokia H&amp;S Supplier Maturity Assessment Process.</td>
<td><strong>Assured</strong></td>
</tr>
<tr>
<td><strong>2018</strong></td>
<td><strong>Health, Safety, and Wellbeing</strong></td>
<td>100% of suppliers delivering high risk activities were covered by H&amp;S Maturity Assessments.</td>
<td><strong>Achieved</strong></td>
</tr>
<tr>
<td><strong>2020</strong></td>
<td>50% of suppliers delivering high risk activity to meet or exceed H&amp;S preferred supplier status.</td>
<td>We are first focusing on getting 100% of suppliers to compliant-level (score 3/5; 89% of suppliers in 2018) and concentrating then gradually to preferred-level (score 4/5).</td>
<td><strong>On track</strong></td>
</tr>
<tr>
<td><strong>2030</strong></td>
<td>100% of suppliers delivering high risk activity to meet or exceed H&amp;S preferred supplier status.</td>
<td>We have an active program ongoing, please see comments on 2018 and 2020 targets.</td>
<td><strong>On track</strong></td>
</tr>
</tbody>
</table>
Ethical business and corporate governance

Our long-standing reputation for acting with unyielding integrity is our most precious asset. Our commitment to upholding the highest principles of business ethics and integrity defines us as a company and distinguishes us from many of our competitors.

Throughout our more than 150-year history, we have nurtured and maintained a culture of high integrity where every employee is held accountable and responsible for upholding our ethical values and for conducting business with unwavering standards of integrity, embracing both values and rules.

**Code of Conduct**

We have a Code of Conduct that is applicable to all our employees, directors and management, as well as a Code of Ethics applicable to the President and CEO, Chief Financial Officer, Deputy Chief Financial Officer and Corporate Controller. Our Code of Conduct sets down the key principles and practices of our ethical business approach to all daily activities and business dealings and provides clear guidance to our employees as well as other stakeholders.

We are committed to following and upholding the laws and regulations in all countries where we operate. The high standards of our Code of Conduct include basic legal guidance and information on key ethical behavior standards. Our Code promotes personal integrity and ethical decision-making in daily work and various business scenarios and protects our valuable reputation.

The Code of Conduct is further enhanced by non-exhaustive summaries of the 14 key business policy statements that provide guidance on proper ethical conduct. The 14 policy statements include: Improper Payments/Anti-Corruption, Conflict of Interests, Fair Competition, Privacy, Dealing with Government Officials, Intellectual Property & Confidential Information, Working with Suppliers, Trade Compliance, Insider Trading, Health, Safety & Labor Conditions, Controllership, Fair Employment Practices, Human Rights, Environment, and operational guidance on third-party screening and corporate hospitality. The complete policies and respective Q&As are made available to our employees.

The Code underpins all conditions of labor regulations and is supplemented and strengthened with human rights policies and procedures that underscore how we aim to ensure fair employment. Equality and respect are fundamental to our company’s culture, where a diverse and inclusive workplace provides opportunities for achievement and growth based on merit. We strictly prohibit any form of discrimination, retaliation, or harassment, including sexual harassment.

In 2018, we launched a new initiative, Respect@Nokia, aimed at raising awareness among our employees and ensuring that all employees give and receive respect, irrespective of their diverse backgrounds and orientation. The campaign also focused on raising awareness that in line with our values, we do not tolerate harassment of any kind, including sexual harassment, in our workplace. The campaign was jointly launched through a video message from our CEO and Chief Legal Officer.

Our Compliance Policy Owner program is a critical element of our overall compliance program. Each of the 14 key compliance policies in our Code is managed by a designated functional expert, who is the identified subject matter expert responsible for monitoring that the company remains compliant with laws and regulations, adapts to changing market conditions and business imperatives, and incorporates evolving best practices standards into their programs so that all employees are aware of the policies, laws, and regulations to which they must abide.

The Code is cascaded to employees via a mandatory Ethical Business Training that requires an acknowledgment and commitment to the Nokia Code. The 2018 Code acknowledgment requirement

**Five simple principles define how our employees are expected to behave:**

- Obey laws and follow policies
- Be fair and honest
- Treat each other with respect
- Declare conflicts of interest and avoid appearance of impropriety
- Report any concerns promptly

Nokia People & Planet Report 2018
5.3 Ethical business and corporate governance

was communicated broadly via intranet resources, emails, social media posts, and line manager notices. The Code is accessible from various resources, including a company mobile app, initially launched in 2015, to reach out to our highly mobile and tech-savvy workforce. The Code is available in 24 languages and publicly available in English, please see our Code of Conduct.

We work closely with licensees to ensure adherence to the same standards of ethical business across all interactions and to help ensure responsible sourcing and globally acceptable labor practices. To this end, we require our licensees to follow strict requirements based on our Code of Conduct, privacy, security, and anti-corruption policies, human rights, trade compliance, environmental policy as well as marketing and product quality requirements.

Leadership engagement, accountability and compliance oversight

Our unceasing commitment to integrity spans the organization vertically from the Board of Directors, through the leadership to employees at every level of the organization, and horizontally from our base in Finland to our far-flung operations in Asia, Africa, Europe, the Middle East, and the Americas.

Our Chief Compliance Officer (CCO) presents separately and independently to the full Board once per year, to the Audit Committee of the Board four times per year, or as needed, and to the Compliance Meeting attendees, which includes GLT members, once per year. The CCO also regularly meets with the Audit Committee in executive sessions without members of senior management present. Our CCO reports solid line to the Chief Legal Officer (CLO), with dotted line reporting to the Board.

The structure of our organization is designed to maximize the effectiveness of the program. The Ethics and Compliance (E&C) organization is matrixed, with dedicated compliance leaders for each of the company’s six regions plus China, which is covered by the Nokia Shanghai Bell (NSB) compliance team. Another compliance team is focused on supporting Nokia’s business groups. This structure ensures that compliance risks are identified and managed both horizontally and vertically. In addition to the dedicated E&C organization, our Legal Team is an integral part of the compliance program and is vested with the responsibility to drive compliance in their daily operations and those of their assigned client groups.

The regional and business compliance program is complemented through other compliance operating forums, such as the Compliance Operation Reviews (CORs) and the Disciplinary Committees where leaders – and not the compliance team – own and are accountable for compliance. CORs are led by the business or country head, with active participation from senior leaders from the finance, HR, services and procurement teams, and are a critical part of our strategy of leadership engagement and ownership in all aspects of compliance. At each level and in each forum, leadership engagement is a critical part of the structure.

Compliance reimagined – 2018

In 2018, we continued to build on the theme of Compliance Reimagined. We executed on ambitious goals and implemented key initiatives supporting these goals throughout the year, including:

• Go Local initiative, which targeted compliance at the grassroots level
• Compliance training sessions, policies, and processes deployed in our Service Companies as well as in Joint Ventures
• Data analytics and monitoring activities incorporated into our Third-Party Program elements to stay ahead of risks
• Comprehensive 360-degree Compliance Risk Assessment, including soliciting employee feedback through an Employee Compliance Survey
• Global deployment of the Nokia Compliance Controls Framework (CCF) and mitigation of compliance risks by addressing identified gaps
• Compliance Operating Reviews, focused on identifying operating compliance risks in collaboration with business teams
• Robust compliance program deployed after a merger or an acquisition – ensuring that new employees were inducted into Nokia’s culture early in the game
• Comprehensive and pertinent training calendar that included online training seminars as well as face-to-face training sessions to raise awareness and sustain the culture
• Anti-corruption risks managed by our specialized Center of Excellence (CoE) with emphasis on strengthening and streamlining policies, processes, and support and
• Year of the How, focused on establishing compliance as a strategic business partner.
5.3 Ethical business and corporate governance

Open reporting – Global Ombuds Program
The Ombuds Program was launched globally in April 2017 and continued to be deployed in 2018 to further strengthen our company’s speak-up culture and reinforce our non-retaliation policy. The vast network of local ombuds leaders actively promotes the program and serves as confidential and neutral resources for employees who have compliance questions, concerns and requests for guidance. The ombuds network is a critical element in preventing, detecting and addressing wrongdoing by expanding the existing channels currently available for raising concerns.

In addition to the program rollout, the Space to Speak awareness campaign was launched globally to spread awareness on the program and the role of local ombuds representatives.

Compliance risk assessment and mitigation
Evaluating ethics and compliance risk is critical to our success. As a result, we have implemented a systematic and structured approach to risk management across our business operations and processes. Key risks and opportunities are primarily identified against business targets, either in business operations or as an integral part of financial planning. These key risks and opportunities are analyzed, managed, monitored and identified as part of overall business performance management with the support of risk management personnel. Risk management covers strategic, operational, financial, and hazard risks and is focused on eliminating risk, as well as managing the key risks that would prevent Nokia from meeting its objectives.

Ombuds Update
Status as of December 31, 2018

Open reporting – Global Ombuds Program
The Ombuds Program was launched globally in April 2017 and continued to be deployed in 2018 to further strengthen our company’s speak-up culture and reinforce our non-retaliation policy. The vast network of local ombuds leaders actively promotes the program and serves as confidential and neutral resources for employees who have compliance questions, concerns and requests for guidance. The ombuds network is a critical element in preventing, detecting and addressing wrongdoing by expanding the existing channels currently available for raising concerns.

In addition to the program rollout, the Space to Speak awareness campaign was launched globally to spread awareness on the program and the role of local ombuds representatives.

Compliance risk assessment and mitigation
Evaluating ethics and compliance risk is critical to our success. As a result, we have implemented a systematic and structured approach to risk management across our business operations and processes. Key risks and opportunities are primarily identified against business targets, either in business operations or as an integral part of financial planning. These key risks and opportunities are analyzed, managed, monitored and identified as part of overall business performance management with the support of risk management personnel. Risk management covers strategic, operational, financial, and hazard risks and is focused on eliminating risk, as well as managing the key risks that would prevent Nokia from meeting its objectives.

Ombuds Update
Status as of December 31, 2018

Open reporting – Global Ombuds Program
The Ombuds Program was launched globally in April 2017 and continued to be deployed in 2018 to further strengthen our company’s speak-up culture and reinforce our non-retaliation policy. The vast network of local ombuds leaders actively promotes the program and serves as confidential and neutral resources for employees who have compliance questions, concerns and requests for guidance. The ombuds network is a critical element in preventing, detecting and addressing wrongdoing by expanding the existing channels currently available for raising concerns.

In addition to the program rollout, the Space to Speak awareness campaign was launched globally to spread awareness on the program and the role of local ombuds representatives.

Compliance risk assessment and mitigation
Evaluating ethics and compliance risk is critical to our success. As a result, we have implemented a systematic and structured approach to risk management across our business operations and processes. Key risks and opportunities are primarily identified against business targets, either in business operations or as an integral part of financial planning. These key risks and opportunities are analyzed, managed, monitored and identified as part of overall business performance management with the support of risk management personnel. Risk management covers strategic, operational, financial, and hazard risks and is focused on eliminating risk, as well as managing the key risks that would prevent Nokia from meeting its objectives.

Ombuds Update
Status as of December 31, 2018

Open reporting – Global Ombuds Program
The Ombuds Program was launched globally in April 2017 and continued to be deployed in 2018 to further strengthen our company’s speak-up culture and reinforce our non-retaliation policy. The vast network of local ombuds leaders actively promotes the program and serves as confidential and neutral resources for employees who have compliance questions, concerns and requests for guidance. The ombuds network is a critical element in preventing, detecting and addressing wrongdoing by expanding the existing channels currently available for raising concerns.

In addition to the program rollout, the Space to Speak awareness campaign was launched globally to spread awareness on the program and the role of local ombuds representatives.

Compliance risk assessment and mitigation
Evaluating ethics and compliance risk is critical to our success. As a result, we have implemented a systematic and structured approach to risk management across our business operations and processes. Key risks and opportunities are primarily identified against business targets, either in business operations or as an integral part of financial planning. These key risks and opportunities are analyzed, managed, monitored and identified as part of overall business performance management with the support of risk management personnel. Risk management covers strategic, operational, financial, and hazard risks and is focused on eliminating risk, as well as managing the key risks that would prevent Nokia from meeting its objectives.

Ombuds Update
Status as of December 31, 2018

Open reporting – Global Ombuds Program
The Ombuds Program was launched globally in April 2017 and continued to be deployed in 2018 to further strengthen our company’s speak-up culture and reinforce our non-retaliation policy. The vast network of local ombuds leaders actively promotes the program and serves as confidential and neutral resources for employees who have compliance questions, concerns and requests for guidance. The ombuds network is a critical element in preventing, detecting and addressing wrongdoing by expanding the existing channels currently available for raising concerns.

In addition to the program rollout, the Space to Speak awareness campaign was launched globally to spread awareness on the program and the role of local ombuds representatives.

Compliance risk assessment and mitigation
Evaluating ethics and compliance risk is critical to our success. As a result, we have implemented a systematic and structured approach to risk management across our business operations and processes. Key risks and opportunities are primarily identified against business targets, either in business operations or as an integral part of financial planning. These key risks and opportunities are analyzed, managed, monitored and identified as part of overall business performance management with the support of risk management personnel. Risk management covers strategic, operational, financial, and hazard risks and is focused on eliminating risk, as well as managing the key risks that would prevent Nokia from meeting its objectives.

Ombuds Update
Status as of December 31, 2018

Open reporting – Global Ombuds Program
The Ombuds Program was launched globally in April 2017 and continued to be deployed in 2018 to further strengthen our company’s speak-up culture and reinforce our non-retaliation policy. The vast network of local ombuds leaders actively promotes the program and serves as confidential and neutral resources for employees who have compliance questions, concerns and requests for guidance. The ombuds network is a critical element in preventing, detecting and addressing wrongdoing by expanding the existing channels currently available for raising concerns.

In addition to the program rollout, the Space to Speak awareness campaign was launched globally to spread awareness on the program and the role of local ombuds representatives.

Compliance risk assessment and mitigation
Evaluating ethics and compliance risk is critical to our success. As a result, we have implemented a systematic and structured approach to risk management across our business operations and processes. Key risks and opportunities are primarily identified against business targets, either in business operations or as an integral part of financial planning. These key risks and opportunities are analyzed, managed, monitored and identified as part of overall business performance management with the support of risk management personnel. Risk management covers strategic, operational, financial, and hazard risks and is focused on eliminating risk, as well as managing the key risks that would prevent Nokia from meeting its objectives.
Our risk assessment program is a dynamic process and the program is implemented through three independent and unique mechanisms:

1. Quarterly Enterprise Risk Management (ERM)
2. Annual company-wide compliance risk assessment exercise to understand potential compliance issues that employees may face and to provide appropriate support to help them deal with compliance risk and
3. Country or entity-specific Compliance Controls Framework (CCF Reviews) – essentially an internally-developed, business-owned process of identifying anti-corruption risks and developing responsive mitigation controls.

Each of these processes provides a unique opportunity to probe more deeply into the business, functional, country and/or entity specific risks. Identified risks are then addressed through a detailed mitigation plan with assigned ownership and accountability. Each item is tracked for timely completion. Each methodology complements the other and using all three vehicles, spread out at different times during the year, ensures that we have a 360-degree view of our processes and are receiving feedback from multiple touch points.

The CCF review is used as part of a compliance package and to enhance engagement, for example: 1. Round table with senior management on exceptional compliance risks faced and how to remediate them. 2. Targeted face-to-face training 3. Encourage open discussion of compliance risks faced and instigate buy-in and

Compliance Control Framework Reviews – The Concept

- Providing guidance on design and evaluation of compliance controls
- A means to reduce compliance risk
- Tool to assess compliance controls over operations and other reporting objectives (anti-corruption/anti-fraud focus)
- Anti-corruption/anti-fraud compliance embedded in local operations
- Enable country organizations as First Line of Defense
- Improve reliability of information for decision-making

4. Demonstrate compliance presence and oversight in dark corners.

In 2018, E&C carried out 22 CCF reviews, including ten country CCF reviews, two Business Group reviews (ASN & India Global Delivery Center), eight Service Companies, and two Joint Ventures.

Gauging effectiveness

In addition to these assessments, we continuously engage with employees through anonymous surveys to gauge the effectiveness and understanding of our compliance program across the workforce. In 2018, we introduced a new Employee Compliance Survey as part of our risk assessment program:

- 16 questions addressing: Tone from the Top, Compliance Program effectiveness, Improper Payments, Conflict of Interest, Data Protection, Privacy, Fair Competition & Trade Compliance
- Delivered by an online tool and responses were anonymous
- 19,876 employees responded and
- Results were overall good – between 82 percent and 96 percent of the responses were favorable.
5.3 Ethical business and corporate governance

Findings from the Survey were integrated into the 2018 Compliance Risk Assessment alongside other inputs (CCF reviews, Compliance Operations Reviews and Internal Audit review results, Compliance investigations, CCT survey results, etc.)

Employee and other stakeholder inputs are actively sought to further develop the company’s program through round-table meetings with business leaders at our sites around the world, as well as inclusion in external presentations to various stakeholder groups. This is shown through the inclusion of ethics and compliance in discussions with key suppliers as part of ongoing training and engagement. We use these multiple feedback channels to drive and enhance the culture of continuous improvement in our compliance program.

On an annual basis, our Internal Audit team also collaborates with the compliance team in audits and through other inquiries that assess the effectiveness of our compliance processes and controls. This included anti-corruption risk reviews covering expense statements, petty cash, bank account access, revenue recognition, selection and use of supplies. The Internal Audit team collaborated to take steps to mitigate all risks identified during these reviews.

And lastly, Internal Audit is called in by the E&C organization to assist with investigations that are financial in nature. These requests are treated with high priority and other work is reprioritized to provide the needed resources, often altering the internal audit plan to address these priorities.

Similarly, Internal Audit also attends the quarterly E&C regional reviews where issues that have been identified through audits are presented and discussed. Internal Audit also involves the E&C organization when ethics-related issues are identified in audits. This may involve potential issues of employee fraud, third party onboarding and/or due diligence, and gifts and hospitality policy.

Compliance training program
Effective and engaging compliance training for all employees is an essential component of our compliance program. We require that every employee completes annual training in ethical business practices, as well as other live and web-based targeted training, on topics such as anti-bribery, competition law, conflict of interest, and privacy.

Annual training plans are created and are based on defined compliance topics of importance, new and/or updated policies, potential risks identified, and any other key changes to law or regulations that need to be addressed.

Course content for both live and web-based training sessions is constantly assessed to ensure that it incorporates best practice standards for ethics and compliance training. All training includes real life scenarios, knowledge checks and links to important company policies, procedures and contacts, where applicable.

In 2018, live training sessions were delivered to business groups, to relevant stakeholders, to regional groups, including country engagement sessions, and to service companies, with over 7,800 individuals receiving face-to-face training in the 236 live training sessions held across the globe.

The Ethical Business Training module is one of the mandatory web-based training courses that was deployed in 2018. This training includes a review of all 14 policy areas in our Code of Conduct including: ethics in the workplace, fair competition and anti-trust, trade compliance, privacy, bribery and corruption, gifts, entertainment and hospitality, conflicts of interest, human rights, environment, equal opportunity, discrimination, and harassment. We achieved 95 percent completion globally by the December 31, 2018 deadline.

Compliance communications program
Compliance communications are necessary to ensure that all employees are knowledgeable about and understand the laws, regulations and policies that apply to them. In addition to formal training, we have developed a robust and comprehensive communication and awareness program to foster a culture of integrity, to enhance compliance awareness, and to ensure adherence to the Code and related policies.

“Wisdom is knowing the right path to take. Integrity is taking it.”
We employ two different approaches for communications:
• Global – communications are distributed to all employees
• Regional – communications are customized to reflect local initiatives and requirements.

The Ethics & Compliance 2018 Communications Plan utilized various communication vehicles to keep the messaging dynamic and interesting, including: town hall meetings, push emails, newsletters, Yammer posts, compliance blogs, a dedicated line manager newsletter, and multimedia training. In addition, the dedicated Ethics & Compliance website consolidates essential compliance resources into one central location and facilitates continuous reinforcement of the company’s commitment to compliance and integrity.

In 2018, we also designed and deployed two engaging, informational videos. Our Open Reporting video emphasized the importance of a speak-up culture and reporting concerns. The video also attempted to demystify the investigations process by explaining what happens after a concern is raised. The Ombuds Program video reminded employees to utilize the growing Ombuds network, letting them know that we truly want to hear the voice of our employees, and it encouraged all employees around the world to feel empowered and comfortable speaking up about compliance.

To support the initiative, core and customized regional activities were planned that were designed to:

• drive awareness of how integrity impacts employees in their everyday work
• promote integrity as a fundamental way of how we conduct business
• lead by example by providing tangible, concrete examples of integrity in the workplace
• engage and enable employees to comply and align with Nokia’s core values

Feedback from the 2018 Integrity Week was exceedingly positive, with robust and global engagement of employees and senior leaders. Local events were held at 90 sites globally with an estimated 7,500 attendees participating in person in the activities held around the globe. The Integrity

<table>
<thead>
<tr>
<th>2018 Integrity Day</th>
<th>Number of Compliance Hero Recipients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of employees who read Chief Compliance Officer’s blog of November 7</td>
<td>Number of Compliance Hero Recipients</td>
</tr>
<tr>
<td>2,288 (as of January 22, 2019)</td>
<td>15</td>
</tr>
<tr>
<td>Number of employee who attended the on-site activities (estimated):</td>
<td>Number of sites that reported on-site activities</td>
</tr>
<tr>
<td>~7,520</td>
<td>90</td>
</tr>
</tbody>
</table>

Integrity Day
In 2018, we hosted a global Integrity Day event, providing a dedicated opportunity to reinforce our core values and commitment to doing business with integrity. The goal of Integrity Day is to engage with employees globally to create awareness around the Code of Conduct, reporting channels, policies and other important compliance initiatives. We do this in numerous creative and interesting ways, reinforcing the message that business integrity is not just a corporate responsibility, but a personal one for every employee.
Day event wrapped up with the announcement of our 2018 Compliance Hero Award Recipients. This program, created in 2017, was designed to recognize employees who uphold and exhibit exemplary ethical values and behavior. In 2018 we received 29 nominations for the award, of which 15 employees were recognized as compliance role models in one or more of the following categories: Speak Up; Challenge; Determination; Respect and Excellence.

**Ethical business and corporate governance**

**Reporting of ethical concerns without fear of retaliation**

It is paramount that we maintain a culture and atmosphere of trust among our employees. This ensures all employees feel comfortable in bringing concerns and potential violations of the Code of Conduct to our attention, without fear of reprisals, retaliation, or negative response. We clearly state in our Code of Conduct that there is zero tolerance for retaliation related to reporting of ethical concerns. Confidentiality is guaranteed.

We offer multiple channels to report ethical concerns, through a dedicated email address, online portal, or via dedicated country-specific phone numbers. We respond to and investigate all concerns promptly and take any necessary corrective actions. All concerns are logged and tracked regularly. Our Helpline is open for employees and external stakeholders. Our Ethics Helpline allows for anonymous reporting.

In 2018, our Ethics & Compliance Office received 887 concerns of which 248 were investigated by our Business Integrity Group as alleged violations of our Code of Conduct and 92 allegations were substantiated with “cause found” after investigations. For 2018, we also implemented corrective actions including 24 dismissals, and 16 written warnings, following these and other investigations. The number of concerns and requests for guidance reported to the Helpline increased by 30 percent from 2017. This increase is largely attributable to the continued efforts by the compliance team to promote a culture of open reporting in the company. Specifically, two concerns were received as alleged violations of our anti-bribery policies, involving third parties, but neither of these concerns was substantiated.

During 2018, we expanded our efforts to encourage employees to use the Ethics Helpline beyond reporting concerns or potential compliance violations. The Helpline also welcomes requests for guidance on ethical dilemmas or questions regarding the application of company policy to particular situations. The result of these efforts was reflected in the increase in the number of reports in 2018.
### 5.3 Ethical business and corporate governance

**Helpline Information:** Email: ethics@nokia.com; Online website: www.nokia.ethicspoint.com; Phone: www.nokiaphone.ethicspoint.com.

#### Number of ethical concerns reported in 2018

<table>
<thead>
<tr>
<th>Type</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflict of interest</td>
<td>55</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controllership</td>
<td></td>
<td>74</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dealing with government officials</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fair competition</td>
<td></td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fair employment (all HR-related concerns)</td>
<td>336</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guidance</td>
<td></td>
<td>186</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human rights</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improper payments</td>
<td></td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intellectual property and confidential information</td>
<td>59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trade compliance</td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wellbeing, health, safety and environment</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Working with suppliers</td>
<td></td>
<td>58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>58</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total number of concerns reported</strong></td>
<td><strong>55</strong></td>
<td><strong>74</strong></td>
<td><strong>186</strong></td>
<td><strong>887</strong></td>
</tr>
</tbody>
</table>

#### Number of investigations by the Ethics & Compliance Office

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>257</td>
</tr>
<tr>
<td>2016</td>
<td>228</td>
</tr>
<tr>
<td>2017</td>
<td>257</td>
</tr>
<tr>
<td>2018</td>
<td>248</td>
</tr>
</tbody>
</table>

#### Number of employees dismissed on grounds of a violation of the Code of Conduct

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>17</td>
</tr>
<tr>
<td>2016</td>
<td>62</td>
</tr>
<tr>
<td>2017</td>
<td>47</td>
</tr>
<tr>
<td>2018</td>
<td>24</td>
</tr>
</tbody>
</table>
5.3 Ethical business and corporate governance

### Ethical business – case examples of reported concerns

<table>
<thead>
<tr>
<th>Issue raised</th>
<th>Our guidance</th>
<th>Actions taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country IT Manager made purchases of phones and computers without POs and for personal gain.</td>
<td>Nokia Code section on Controllership emphasizes that an employee must not misrepresent financial records, including falsifying expense reports.</td>
<td>The allegations were substantiated and employee was terminated for cause.</td>
</tr>
<tr>
<td>Employee (on last day of employment) was believed to have downloaded Nokia confidential and proprietary information for non-Nokia uses.</td>
<td>Nokia's confidential, proprietary, and trade secret materials are among its most valuable assets. Theft, misuse or misappropriation of Nokia's intellectual property is both a violation of company policy and – in many countries – a violation of the law.</td>
<td>The allegations were substantiated and Nokia took recovery action against the individual.</td>
</tr>
<tr>
<td>Alleged conflict of interest between Nokia employees and subcontractor that was paid several unusual one-off payments.</td>
<td>Nokia Code section on conflict of interests states we act in the best interests of Nokia and use Nokia property and resources primarily for Nokia's benefit.</td>
<td>The COI allegations were not substantiated; however, management visibility over certain cost centers was improved.</td>
</tr>
<tr>
<td>Previously blacklisted vendors secured subcontractor engagements with contractors hired by Nokia – in an attempt to circumvent the supply chain blacklist.</td>
<td>Nokia Code section on Working with Suppliers makes clear our expectation that suppliers be qualified to Nokia standards, approved for use, and share the values expressed in our code.</td>
<td>The allegations were substantiated and future supplier contracts modified to contain a clause prohibiting recurrence and for compliance visibility to subcontractors used by Nokia vendors.</td>
</tr>
</tbody>
</table>

Above are anonymized illustrative examples of investigations carried out in 2018 by our Business Integrity Group.

In 2018, there were no significant fines or non-monetary sanctions for non-compliance with laws and regulations related to anti-corruption, product health or safety and security, environment, data privacy, export control laws or tax payments.

**Anti-corruption, Center of Excellence & Third-Party Program**

As part of our efforts to ensure continuous improvement, in 2017 we had launched a dedicated Anti-Corruption Center of Excellence (COE). The mandate of the COE is to efficiently manage the sales third-party onboarding processes, using a risk-based approach; review and approve gifts, entertainment, hospitality, donations, and sponsorship requests and related monitoring, and engage in data analytics activities.

In addition to driving awareness through training and communications, the COE employs two critical tools to implement the company’s anti-corruption program. First, requests to pre-approve gifts, hospitality, sponsorships and donations extended to external parties are entered by employees into the online Gifts, Travel and Entertainment (GTE) Tool in accordance with relevant procedural requirements. Second, all requests to onboard sales third parties are entered in the online Third-Party Screening Tool (TPST) in accordance with relevant procedural requirements.

We employ a multi-faceted approach to anti-corruption issues. We have clear and unequivocal policies concerning improper payments, facilitation payments, gifts and hospitality, sponsorships and donations, and other risk areas. We carry out training and regularly communicate to our employees regarding risks, and we review these risks and our mitigation measures with the company’s senior leadership and Audit Committee.
We carefully screen and monitor any commercial third-party representatives engaged to act on our behalf and we demand the same high standards of conduct from them. We conduct periodic audits and risk assessments to ensure that we identify and respond to anti-corruption risks. We expect employees to ask questions and raise concerns whenever they believe there is a potential law or policy violation, and we investigate all such concerns in a prompt, thorough and objective manner. When an investigation confirms a violation, individuals are held accountable.

To properly address anti-corruption related issues, the company has developed and implemented a global Improper Payments program that reaches all of our employees, as well as our business partners. The program is comprehensive and consists of several complimentary anti-corruption policies, procedures, processes and guidance designed to prevent the offering, giving, or receiving of improper payments, with emphasis on interactions with government officials. Such payments include facilitation or so-called “grease” payments, improper gifts, entertainment, gratuities, favors, donations or any other improper transfer of value.

The company works closely with its third parties (both on the sales side and purchasing side) to encourage adherence to the same standards of ethical business across all interactions and to help ensure responsible sourcing and globally acceptable labor practices. We actively engage with our distributor partners, based on a foundation of mutual trust, helping them build their own robust compliance programs and at the same time establishing lasting relationships that extend beyond developing business.

Our program is designed to ensure that we only engage reputable commercial third parties who share our unwavering commitment to ethics and integrity and meet our stringent due diligence standards.

We require our sales third parties to acknowledge our Commercial Third-Party Code of Conduct (available in eight languages) during the onboarding process, after having gone through a thorough screening exercise. It relays Nokia’s expectations to its commercial third parties on ethical conduct and covers key compliance risks under the three main topics of: Legal and Regulatory Compliance (anti-corruption, trade compliance, insider trading, anti-trust, anti-money laundering); Ethical Business Practices (conflict of interest, privacy, intellectual property, record-keeping, confidential reporting); and Environmental and Social Regulations (fair employment, environment, health and safety and human rights).

We also follow a strict no agents rule that prohibits the use of commercial agents in virtually all of our commercial dealings, other than in exceptional cases or where required by law. We believe that every commercial partner we engage must bring tangible and material value. Agents who broker deals or provide only consultancy services in a deal are strictly prohibited from working on our behalf. This reduces the risk of corruption considerably.

We drive awareness of the specific requirements of relevant procedures and processes through global communications and targeted trainings delivered by our Regional and Business Compliance Counsels, not only covering our own employees, but also our sub-contractors and customers, where necessary.

**Competition laws**
Our competition law compliance program aims to ensure that we meet our goal of full compliance with applicable competition laws. We compete fiercely, but fairly. We are committed to complying with competition laws everywhere we do business. The competition compliance program consists of an implementation and monitoring framework, systematic awareness raising and mechanisms for incident reporting and management. Competition law compliance is integrated into our Code of Conduct through the competition policy statement and manifested in our group-wide Competition Law Compliance Policy. The policy statement highlights some key issues for employees to keep in mind and watch out for in the field of competition law.

**Competition law compliance policy**
Competition law is covered as one important compliance area in our annual Ethical Business Training that is mandatory for all employees. In addition to this mandatory training, Nokia arranges other types of training sessions and awareness-raising activities to ensure that relevant employees...
Ethical business and corporate governance

5.3

are familiar with competition rules. We arrange for example web-based and face-to-face training exercises and refreshers for targeted employee groups in need of deeper understanding of applicable competition rules and potential risk areas.

In 2018, targeted competition training sessions were provided, for example, to our compliance leaders and to the L&C organization. These covered many competition areas including dealing with competitors and collaboration in tenders, procurement, and implementing our global dawn raid guidelines. Our group-wide Competition Law e-learning, revised and launched in 2016 to reflect the company reorganization, is required for all our employees to whom competition law may be relevant in their work.

The Competition Law e-learning provides employees with an overview of the basic competition rules on dealing with competitors, suppliers and other business partners, and the abuse of dominance. It provides some typical risk scenarios and covers different practical situations and case examples, thereby providing an understanding of how competition law may play into the daily work in different circumstances.

The Competition Law e-learning, the Competition Law Compliance Policy, along with some specific competition compliance guidelines and materials, as well as recorded training sessions and presentations, are available to our employees through the company intranet. There is a dedicated site for the competition compliance program under Fair Competition.

World's Most Ethical Award

We were honored in early 2019 for the second consecutive year, and third time overall, by the Ethisphere Institute as one of the World's Most Ethical Companies¹, owed to our strong compliance program, culture, and bold vision for the future. The award is given annually by Ethisphere, a leading organization for corporate ethics and compliance, to a small and select group of companies, following a rigorous evaluation process screening the company's policies, processes, social responsibility, governance, and compliance culture. Having weathered unprecedented technological change and absorbed companies with varying commitments to ethical practices, we have literally raised the bar for integrity in our field. In 2019 only four telecom companies globally were honored with this award.

¹ World's Most Ethical Companies” and “Ethisphere” names and marks are registered trademarks of Ethisphere LLC.

Responsible advertising

Advertising at our company must be built on a clear and accurate messaging framework, as set out in our visual and verbal guidelines, with pragmatic statements, grounded in fact, with real proof points, and reasons to believe in Nokia. The use of false or deceptive messages, ambiguity, or aggressive sales techniques are strictly forbidden and against our Code of Conduct and our brand guidance.

“As there is a growing movement and awareness regarding trust and integrity in today’s businesses, Nokia is pleased to once again be recognized as one of the World’s Most Ethical companies. It has long been part of the Nokia way to treat every business relationship according to the highest ethical standards.”

Rajeev Suri, President and CEO, Nokia
We are committed to the principles of the Universal Declaration of Human Rights and the United Nations’ Global Compact, and we encourage our suppliers and business partners to share these values.

We endorsed the United Nations Guiding Principles on Business and Human Rights in 2011. On balance, we believe that connectivity and the technologies we provide are a social good that can support human rights by enabling free expression, access to information, exchange of ideas, and economic development. Freedom of expression is crucial to the development of knowledge and understanding and the access to information and ideas is essential to transparency and accountability.

Our Code of Conduct and Human Rights Policy guide our human rights work and activities. The most direct human rights risks related to our company and business involve the potential misuse of the technology we provide, particularly where it relates to lawful interception capabilities and activities by governments that relate to the network infrastructure equipment that we design, produce and support for telecom operators. Our Human Rights Due Diligence process helps ensure via our sales interface that human rights are not infringed upon through the misuse of the technology we provide to our customers.

The ICT supply chain is multi-layered and diverse as we operate in many countries, and we recognize the risk that our employees, partners or agents may take actions that contradict our Code of Conduct or that customers and suppliers may similarly violate these principles, which could also have an adverse impact on our reputation, brand, or financial position. We therefore employ a range of processes and procedures to mitigate these risks. Our work with our supply chain is discussed in more detail in the Responsible Sourcing section of this report.

The table above helps readers of this People & Planet report to find information on specifically mentioned human rights topics in relation to the requirements of the French duty of vigilance law. At this time, similar regulatory discussions are ongoing in other countries.
Respecting the right to privacy and freedom of expression – preventing the misuse of technology

Technology and services will have an even greater role in our daily lives as the world moves into what some call the Fourth Industrial Revolution.

5G, IoT, Cloud, AI and other newer technologies will enable digital lives, where billions of people and things are connected. The benefits are many – faster communication, access to social and economic opportunities, instant information and ideas, as well as social and environmental benefits. New technologies can make the world more inclusive.

However, we recognize that technology can be misused and as a communications technology equipment vendor, we have a responsibility to ensure our technology is not used to limit or infringe on human rights. We continue to work both in our own company and with the broader stakeholder community to drive the dialog on balancing the privacy rights of the individual with the increased need for security for both individuals and societies. For example, although our use of AI and machine learning is principally aimed at improving network performance and maintenance efficiency, we have proactively rolled out internal employee training programs that include internal and external expert presentations on AI in relation to privacy, data security, and human rights issues. We also have in place a Privacy by Design program across our product portfolio.

Our human rights due diligence

We carry out rigorous Human Rights Due Diligence (HRDD) investigations to mitigate potential risks posed by the misuse of our technology. The HRDD process is defined as a non-commercial cross-functional investigative process which is used to identify the potential risk of human rights violations through the misuse of our technology, while also attempting to identify ways to mitigate these risks to ensure compliance to our Human Rights Policy. Our approach provides a three-dimensional model to help identify potential risk cases early in the process and trigger the required HRDD investigation and senior-level approval/denial review where necessary. Internal awareness and understanding of the potential human rights issues associated with the misuse of technology, as well as understanding of the Human Rights policy and HRDD process is paramount to ensuring our sales teams have the right knowledge to flag cases early in the sales process. Gatekeeping, checkpoints and triggers for the process are reviewed and where needed improved on an ongoing basis.

Our experience from HRDD case reviews over the last two years indicates a potentially rising trend in the so-called dual use of standard technology. When conducting risk assessments, we strive to...
make a deliberate effort to focus on the operator or government’s ultimate use of the technology (referring to this as the “use case”). Simply monitoring lists of individual product sales items is not a sufficient measure to adequately assess the intended use of the technology provided.

**Transparency – a must to strengthen the overall dialog on human rights**

Government requests for network shutdown or content blocking are received by telecom operators in many countries but are not received as such by network equipment vendors. Our customers, many of whom publish transparency reports on such requests, may on occasion come to us to implement a functionality in our equipment to comply with such requests, or in rare cases the authorities may be looking for equipment vendors to implement specific technical capabilities or solutions for example for direct access. We state clearly our position on these requests in our Human Rights Policy – we do not pursue business directly with intelligence agencies concerning such surveillance functionalities. Furthermore, we provide only passive lawful interception capability to those customers who have a legal obligation to provide such service as part of their license to operate – an obligation that is common worldwide for nearly all telecoms operators. This means we do not provide services or products related to post-processing, storage or analysis of interception data.

Working with others in our industry, we continue to call for increased transparency from governments related to their surveillance activities and clarity on the laws and regulations governing these topics. We continue to actively engage with the industry, civil society, academia and authorities on achieving balance between the need for personal security and the rights to privacy and freedom of expression as fundamental human rights.

**Commitment to external assessment**

In 2018 we began the preparation process for our commitment to the Global Network Initiative (GNI) to undergo an external Human Rights assessment. We are a member of the board of GNI group of companies, civil society organizations such as human rights and press freedom groups, investors, and academics working together to protect and advance freedom of expression and privacy in the ICT sector.

As an initial step towards the GNI assessment, in 2018 we undertook an internal Human Rights Impact Assessment (HRIA) conducted by The Business and Human Rights Group (The BHR Group), a consultancy focused on human rights issues in the technology sector. The BHR Group worked closely with our human rights team in its preparation. The executive team at Nokia is the initial intended audience. The executive summary is available online.

In late 2018, we also began the planning and pre-assessment work for the full GNI external human rights assessment against the GNI Guiding Principles which can be found at globalnetworkinitiative.org/gni-principles. At the time of publishing this report the GNI assessment process is in the final stages of reporting to the GNI board. We look forward to sharing more information in the near future.

**Increasing transparency on the overall narrative**

In this year’s report we have again included new anonymized case examples from our Human Rights Due Diligence work in 2018 providing insight and examples on the robustness of our HRDD as well as showing both GO and NO GO sales cases. We believe these real case examples support greater transparency and help to drive the dialogue and narrative further, rather than simply reporting numbers of cases. They also serve to emphasize the importance of looking at the use case rather than a simple list of products.
### Human Rights Due Diligence anonymized case examples

<table>
<thead>
<tr>
<th>Case Example 1</th>
<th>High Risk Country</th>
<th>Governmental entity</th>
<th>Request</th>
<th>HRDD investigation</th>
<th>HRDD decision</th>
<th>Policy Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>To provide drones equipped with cameras for a Governmental transport authority for traffic safety purposes.</td>
<td>HRDD recognized the potential vulnerability for misuse for illegitimate surveillance purposes of camera-mounted drones. However, it was determined that in the proposed project (i) the Government end-user was exclusively focused on road and traffic governance and, in particular, had no duties or authority related to intelligence or law enforcement, and (ii) the cameras included in the project scope were not advanced enough to be well suited for surveillance (e.g., they could not be used to zoom in on license plates or in support of facial recognition technology). Consequently, taking account of country risks specifics, the nature of the end-users, and the technical capabilities of the equipment, the risk of the solution being misused for purposes other than legitimate traffic monitoring and road safety was determined to be very low.</td>
<td>GO</td>
<td>Nokia will provide communication systems and standard networking capabilities to governmental customers for purposes such as public safety, railway communications, and smart city enablement. We will not, however, pursue business with intelligence agencies or similar institutions involving or relating to active surveillance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case Example 2</th>
<th>High Risk Country</th>
<th>Governmental entity</th>
<th>Request</th>
<th>HRDD investigation</th>
<th>HRDD decision</th>
<th>Policy Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>To provide a private 4G/LTE public safety network for Government use, including by law enforcement and intelligence agencies.</td>
<td>HRDD investigation determined that while the procuring entity and some end-users of the public safety network would be domestic intelligence agencies (potentially raising concerns given the human rights risk profile of the country), the project scope would not include any sensitive products or items that would provide any additional or enhanced surveillance capabilities with regard to existing commercial networks in the country. The closed network requested to be supplied would be used exclusively by national security related agencies and units for their internal communication and would not be connected to any networks open to the public. As a condition for engaging in the project, a specific signed certification would be obtained from the procuring agency confirming the nature and purpose of the network.</td>
<td>GO (with conditions)</td>
<td>Nokia will not knowingly provide technology or services for the purpose of limiting political discourse, blocking legitimate forms of free speech, or otherwise contributing to activities that are not consistent with internationally recognized human rights standards. Nokia will provide communication systems and standard networking capabilities to governmental customers for purposes such as public safety, railway communications, and smart city enablement. We will not, however, pursue business with intelligence agencies or similar institutions involving or relating to active surveillance.</td>
</tr>
<tr>
<td>Country</td>
<td>Requestor</td>
<td>Request</td>
<td>HRDD investigation</td>
<td>HRDD decision</td>
<td>Policy Principle</td>
<td></td>
</tr>
</tbody>
</table>
|--------------|--------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| Case Example 3 | Extreme Risk Country          | A non-governmental private entity                                        | To provide a location-based monitoring enhancement feature to be activated in specific mobile network cells. The requested solution would enable the monitoring of the location of all subscribers connected to a given cell in a mobile network. The solution would track the location of all subscribers within the given cell (i.e. it would not be activated by/targeted at individually selected user or device identifiers); however, it would only be implemented in specific cells (and not across any full network). The solutions would relay the required information to the standard 3GPP interfaces, and would not involve any features related to storing, analyzing, or post-collection processing of the information. Such a solution could be used, for example, to enable quick responses to unforeseen safety incidents in locations such as airports in situations where ID-based targeted tracking would not be possible within the required time to prevent serious injury to people or damage to property. HRDD further determined that the feature was a mandatory requirement for mobile operators in the relevant country. Furthermore, since the solution would be limited to selected cells, it would not enable indiscriminate mass surveillance or other large-scale monitoring activity. Conversely, the use case for specific safety sensitive locations such as airports was justified and could be effectively implemented through the requested solution. | GO            | Nokia will provide passive lawful interception capabilities to customers who have a legal obligation to provide such capabilities. We will not, however, engage in any activity relating to active surveillance technologies, such as storing or analyzing of intercepted data. |
| Case Example 4 | High Risk Country              | Local telco operator                                                    | The request was twofold with the aim of providing end-to-end lawful intercept via two independent solutions. 1 Standard passive 3GPP/ETSI compliant lawful intercept capabilities for fixed and mobile networks in the telco network 2 Active monitoring centre for Law Enforcement agency  
1 Nokia does provide standard passive 3GPP/ETSI compliant lawful intercept capability to customers who have a legal obligation to provide such a service. This part of the request is acceptable and within our Human Rights Policy. 2 The second part of this request included a monitoring center for the Law Enforcement agency. Given that Nokia does not, by way of policy, sell monitoring centers, nor any support or facilitation related to the implementation of monitoring centers (regardless of location or country), the request to supply a monitoring center was immediately declined | GO (passive standard lawful intercept) NO GO (active monitoring center) | Nokia will provide passive lawful interception capabilities as a feature of Nokia telecommunications products to customers who have a legal obligation to provide such capabilities. We will not, however, engage in any activity relating to active surveillance technologies, such as storing or analyzing of intercepted data. Nokia will seek to prevent the sale of our products and services in cases where we believe there is a significant potential that those products or services could be used to infringe human rights. |
The integrity of our supply chain is a critical but complex component of our own reputation and we work hard to collaborate with both customers and suppliers to drive transparency, sustainability and good ethical and business practice in the supply chain.

We put in place and communicate the processes, requirements, programs, procedures and policies to mitigate supply chain risks wherever possible. We work with our suppliers to remedy, develop and build capability to enable a more sustainable and transparent ecosystem. We engage with our customers to drive improvements and share knowledge and experience.

We have three broad categories of suppliers:
1. Hardware suppliers which cover the materials that go into our products
2. Services suppliers which we offer to customers such as network planning, installation and maintenance and construction of the networks we supply and
3. Indirect suppliers which provide the goods and services we buy to conduct our business, (IT hardware and software, logistics, consulting, financial, legal, marketing and so on.

The majority of our manufacturing suppliers are based in Asia, whereas our services suppliers are located around the world.

In 2018, we had business with approximately 14,000 suppliers, 80 percent of our total supplier spend was distributed across approximately 450 suppliers. Our final assembly included our own factories in Finland, India and Poland as well as Flextronics, Foxconn, Jabil and Sanmina supplier sites.

Our Supplier Requirements are communicated to our suppliers as part of our supplier contracts, and we expect our suppliers to commit to these as part of their contractual obligations. An overview of those requirements can be found on our website. The requirements cover social, ethical and environmental issues. In addition, we have detailed appendices covering environmental requirements including Nokia Substance List applicable for hardware suppliers and health and safety for services suppliers.

We expect our suppliers to ensure they have in place the necessary management systems, resourcing, and a code of conduct that in practice show their commitment to good labor practices and working conditions, respect for human rights, and good ethical business conduct. We further expect and encourage our tier 1 suppliers to apply and cascade the same standards to their own suppliers. Our company purchasing procedures are strictly applied in our relationships with existing suppliers and whenever we engage with potential new suppliers.

Transparency and compliance requirements are firmly applied to all supplier relationships, and gifts or entertainment are neither given nor received beyond nominal value items. We investigate and qualify all suppliers according to our standards and practices, requiring them to comply with all applicable laws and regulations, and show they share the values stated in our Code of Conduct.
Brief overview of supplier base management and corporate responsibility (CR)

Nokia Code of Conduct

Supplier selection & contracting

Supplier qualification

Supplier management

Request for Information (RFI)
- HSE and CR elements
- Anticorruption Due-Diligence

Contractual Agreement main clauses + Nokia Supplier Requirements
& Environmental appendix

Introduction to Nokia Standards
Such as work at height, road safety, electrical

Category Strategies & performance requirements
For preferred, allowed, restricted suppliers

Monitoring Compliance
- EcoVadis: preferred and allowed suppliers
- CDP Climate change: energy intense suppliers (TOP 500)
- CDP Water security: water intense suppliers (TOP 150)
- Health & Safety maturity assessment: all suppliers with high risk activities. Includes also environmental assessment.
- Responsible/Conflict minerals: all 3TG suppliers, spend above 500K
- On-site CR audits: based on country, industry, type of activity, stakeholder concern, results of desktop monitoring.

H&S Consequence Management

Improvement and Capability Building
- Improvement plans (CAPS)
- Webinars
- Onsite workshops in high risk countries
- Guidance materials
- Nokia Learning Academy

Supplier Performance Evaluation (SPE)
Affect supplier strategic status or phase-out

Supplier Risk Profiling
Country, industry & type of activity, business volume

Brief overview of supplier base management and corporate responsibility (CR)
Key figures of our supplier onsite audit program related to sustainability

<table>
<thead>
<tr>
<th>Audit type</th>
<th>Corporate Responsibility audit</th>
<th>Supplier Requirements audit</th>
<th>Supplier H&amp;S maturity assessment</th>
<th>Conflict Minerals audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Human and labour rights, health and safety, environment</td>
<td>CR elements covered as part of entire NSR sets of elements</td>
<td>Health &amp; safety elements</td>
<td>Conflict minerals scoping, due diligence and risk management</td>
</tr>
<tr>
<td>Targeted suppliers</td>
<td>All</td>
<td>All</td>
<td>High risk services</td>
<td>Production (hardware)</td>
</tr>
<tr>
<td>Typical duration</td>
<td>1–2 days</td>
<td>1–2 days, CR few hours</td>
<td>3–4 hours onsite</td>
<td>1 day</td>
</tr>
<tr>
<td>Number of audits in 2017</td>
<td>72</td>
<td>47</td>
<td>900+ (cumulative)</td>
<td>10</td>
</tr>
<tr>
<td>Number of audits in 2018</td>
<td>75</td>
<td>38</td>
<td>~1 400 (cumulative)</td>
<td>10</td>
</tr>
</tbody>
</table>

Overview on types of suppliers addressed through our CR programs
- Over 99 percent of relevant supplier base is covered by Supplier Health and Safety Maturity Assessment.
- Over 46 percent of supplier spend is covered by CDP supply chain climate change program.
- 98 percent of relevant supplier spend is covered by Conflict Minerals program.
- 58 percent of supplier spend is covered by EcoVadis sustainability assessments.
- 100 percent of supplier spend is covered by the Request for Information (RFI) process, related to anti-corruption due diligence, health and safety, and overall sustainability.

For on-site audits we do not measure the percentage as audits are risk-based.

Global supply chain related risks are identified as part of our materiality analysis and Enterprise Risk Management. We also carry out more in-depth analyses to determine all risks related to supplier activities. We take the outcome of these analyses and include them in our category strategies, noting the nature, magnitude, and monitoring as well as performance requirements for these risks. Our procurement teams revisit our category strategies annually. Our risk approach also takes into account the location of the supplier and the business context. We have both detailed KPIs and public global targets directly related to our supply chain activities. Suppliers and other externals also have the opportunity to raise any concerns through our Ethics Helpline. In 2018, out of the total 887 concerns raised via the Helpline, 58 cases related to working with suppliers (40 in 2017). 24 percent of these cases were reported by third party vendors. Read more on raising concerns on page 90 under the Ethics and Compliance.

Monitoring, assessment and auditing
We run assessments with our supplier network regularly to support them in meeting our ethical standards and improving performance where necessary. We monitor our suppliers through a variety of methods, of which the most important are:

Our Nokia supplier requirements audits
Our general audit covers the full set of supplier requirements, and of which corporate responsibility requirements are a subset. We commonly use this type of audit with new high-risk suppliers or when a supplier has seen a significant change in its business situation such as country location change.
Labor conditions and environmental management - in-depth audits

We conduct specific corporate responsibility in-depth audits on our existing suppliers and align with SA8000 methodology in audit implementation. The audits include not only document reviews, interviews with managers and employees, and site visits, but also inspections of facilities, production lines, and warehouses.

In addition, we continue to use EcoVadis sustainability assessments to review the environmental, labor, health, safety, ethics, and sustainable procurement management systems of our suppliers through a tailored questionnaire and supporting document reviews. We require suppliers to achieve at minimum a satisfactory score on EcoVadis and follow up with suppliers whose score is below satisfactory.

In 2018, we had 74 percent (71 percent in 2017) of suppliers on EcoVadis with a satisfactory performance score. We request that EcoVadis scorecards are renewed every 2 years.

In 2018, we implemented 364 (393 in 2017) supply chain audits which included 75 on-site audits on corporate responsibility topics; 38 were on-site audits against our full set of supplier requirements and 251 suppliers were assessed using the EcoVadis scorecards.

In 2018, we spent 190 auditor days conducting corporate responsibility in-depth audits (187 in 2017) at 75 supplier sites (72 in 2017). Countries covered by these audits were: Cameroon, China, Colombia, India, Malaysia, Mali, Mexico, Myanmar, Peru, the Philippines, Senegal and Togo and reached a total of around 49,000 supplier employees.

We found 764 instances of non-compliance of which 378 related to health and safety, 76 related to environment. Based on the findings, we made 1,129 recommendations for improvement, and these are being addressed through corrective action plans. See examples on the following page. As part of the 75 audits, seven of the audits were conducted through our customers’ Joint Audit Cooperation (JAC) framework.

Audit closure is a continuous challenge – our target is to close CR onsite audit findings within six months of the audit. In 2018, timely closure of audits stood at 52 percent. We realize this must be improved and will make increased efforts to achieve a higher percentage closure going forward.

The table is based on 75 CR in-depth audits conducted in 2018.

<table>
<thead>
<tr>
<th>Category of Findings</th>
<th>Instances of non-compliance</th>
<th>Number of potential risk areas identified</th>
<th>Total number of recommendations for improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child labor (proof of age documents missing)</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Forced labor (contract agreement issues/fine/ deduction etc.)</td>
<td>4</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Health &amp; safety</td>
<td>378</td>
<td>178</td>
<td>556</td>
</tr>
<tr>
<td>Freedom of association and right to collective bargaining</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Discrimination</td>
<td>6</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Disciplinary practices</td>
<td>10</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>Working hours</td>
<td>51</td>
<td>11</td>
<td>62</td>
</tr>
<tr>
<td>Remuneration</td>
<td>54</td>
<td>22</td>
<td>76</td>
</tr>
<tr>
<td>Management systems</td>
<td>180</td>
<td>125</td>
<td>305</td>
</tr>
<tr>
<td>Environmental management system</td>
<td>76</td>
<td>23</td>
<td>99</td>
</tr>
<tr>
<td>Total</td>
<td>764</td>
<td>365</td>
<td>1129</td>
</tr>
</tbody>
</table>
### Examples of identified non-compliance and actions taken

<table>
<thead>
<tr>
<th>Category</th>
<th>Non-compliance identified</th>
<th>Actions taken by supplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forced Labor</td>
<td>The proportional payment of the cost of the course / seminar / training is made in case of labor resignation within the following six months from the training.</td>
<td>This finding on forced labor is in the process of closing with Nokia's recommendation that paying back of the training course by the employees shall be stopped/not practiced in cases where the training is a necessity for executing the job a person is assigned to.</td>
</tr>
<tr>
<td>Remuneration</td>
<td>Workmen’s compensation benefit is not in place.</td>
<td>The workmen compensation benefit was issued to employees.</td>
</tr>
<tr>
<td>Health &amp; Safety</td>
<td>Health &amp; Safety Hazard Identification and Risk Assessment is not done yet.</td>
<td>Health and Safety Hazard Identification and Risk Assessment were completed throughout the business units. Control measures have been put in place.</td>
</tr>
<tr>
<td>Working hours</td>
<td>Excessive overtime work observed for employees and there is no evidence of compensating the overtime work performed.</td>
<td>Working time ensured on a monthly basis jointly with Nokia though proper recording with assigned responsible person for the same so that the working time should not be exceeding the total manhours as per statutory requirement. Arrangements were done to change in shift timings where necessary. Additionally: 1. Supplier has plan to approach Nokia to share the projection for 15 days in advance to ramp up shift roster and train people to handle additional work volumes and reduce overtime hours. 2. Supplier has established a policy of no overtime work and the relevant employees, staff and supervisors were communicated and trained on the requirements related to overtime work.</td>
</tr>
<tr>
<td>Management systems</td>
<td>Employment contracts were not complete (including e.g. amount of working hours and total wage and benefits) for all sampled employees. Former contract workers who were changed to regular employees had just a “notice of change on employment status”. Also employees with long working history in the company had very generic clauses in their contracts. Contracts were also not signed on all pages.</td>
<td>Update was done to current procedure indicating that all regular employees should have an employment agreement indicating working hours/salary/NDA for client/supplier and customers and with a signature on all pages.</td>
</tr>
<tr>
<td>Environmental management system</td>
<td>There is no environmental impacts and aspects analysis conducted yet. Inventory of the waste is not maintained. There is no improvement program for the identified environmental aspects such not targets set for waste reduction and reduction for the usage of energy.</td>
<td>Supplier started a program of identification of the environmental aspects and measurement of environmental impacts such as waste and energy usage to start a PDCA improvement cycle on these.</td>
</tr>
</tbody>
</table>

This table is based on 75 CR indepth audits conducted in 2018.
### Responsible sourcing

**Capability building – driving improvements**

Additionally, we ran 11 training workshops for suppliers operating in high-risk countries such as Cameroon, China, Colombia, India, Malaysia, Mali, Myanmar, Mexico, Peru, Senegal, and Togo. In 2018, we organized online trainings on conflict-free sourcing and climate change, and we arranged face-to-face training workshops establishing improvement plans and actions for 393 suppliers. Please refer to the diagram: Supplier participation in Nokia sustainability workshops and webinars.

**Climate impacts – helping suppliers reduce and report**

All our suppliers, except those with very low environmental impact, are required to have a documented Environmental Management System (EMS) in place. For key suppliers and for those with greater impacts, we require certification to ISO 14001, which we track through our audits and assessments.

We jointly create environmental improvement programs in order to improve our upstream Scope 3 emissions reporting through the CDP Supply Chain Program (overall Scope 3 equals all indirect emissions that occur in our value chain, including upstream and downstream). We encourage our key suppliers to report their climate impacts and set carbon reduction targets through CDP and work with them to build improvement programs.

In 2018, 314 of our key suppliers, an increase of 22 from 2017, representing 46 percent of our total procurement spend, responded to the CDPs.

### Supplier participation in Nokia sustainability workshops and webinars

![Diagram showing supplier participation in workshops and webinars over years 2015 to 2018.]

### Supplier climate disclosure figures

<table>
<thead>
<tr>
<th>Category</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppliers disclosed data, &gt;50% of Nokia spend</td>
<td>314</td>
</tr>
<tr>
<td>Suppliers purchased renewable energy</td>
<td>129</td>
</tr>
<tr>
<td>Suppliers engaged their own suppliers</td>
<td>143</td>
</tr>
<tr>
<td>Suppliers reported reduction (178 thanks to us) and have active targets for emission reduction</td>
<td>247</td>
</tr>
<tr>
<td>Suppliers reported GHG emissions (Scope 1/2)</td>
<td>211</td>
</tr>
<tr>
<td>Highlighted collaborative opportunities with us</td>
<td>63</td>
</tr>
</tbody>
</table>

- Total CO\(_2\)\(_e\) reduction: 15 million tCO\(_2\)\(_e\)
- Total € saved: EUR 637 million
request to disclose their climate performance information. Of these 247 disclosed their carbon emissions (an increase of 33 from 2017) and 187 also provided emission reduction targets (an increase of 34 from 2017). The total saving from these carbon reduction initiatives was 14.6 million metric tons CO₂e and around USD 726.3 million during the course of the year.

It should also be noted that 143 suppliers engaged their next tier in CO₂ reporting. In addition, 118 of our suppliers calculated a Nokia allocation of their emissions based on the products and services we purchase from them and 88 suppliers provided emissions intensity data. Using a hybrid methodology for calculation, based on supplier information for Scope 1 and 2 emissions, our emissions with participating suppliers totaled 2.1 million metric tons of CO₂e. By scaling up the allocated emissions to 100 percent of our suppliers, we estimated our scope 3 emissions from our supply chain to be approximately 5.3 million metric tons of CO₂e.

Water – resource management

2018 was the first year of active engagement with our suppliers on the efficient use of water. We have identified supplier categories where water may be a material risk and have begun to address these suppliers with a water assessment program. 150 of our suppliers have already disclosed their water data. More information on our activities concerning water management can be found in the water section of the Protecting the Environment chapter on pages 80–82.

Developing Health & Safety Maturity

We carefully track working conditions as a key component of our sustainability approach to our supply chain. We place special emphasis on health and safety as our supply chain includes equipment installation and maintenance contractors who spend much of their time working at height, in confined spaces, and driving long distances. Armed with the necessary training, we endeavor to ensure these contractors are aware of the potential dangers associated with their work and have and use the appropriate safety equipment. We also augment our health and safety guidance with standards concerning road safety, work at height and working with electricity, which is further covered in our supplier workshops.

At the end of 2018, of those suppliers who provide us with high risk activities, (working at height, transportation, and electrical work), 100 percent were covered by our health and safety maturity assessments (on-site evaluations conducted by our regional health and safety professionals). 89 percent (an increase of 8 percent from 2017) of assessed suppliers met H&S compliant supplier status. Those not meeting the requirement were recommended for phase-out or for thorough improvement where we had no alternative choice. For example, in some developing countries we do not have suppliers capable of meeting our requirements, and we need to work hard to help them improve while putting strong supervision in place.

While strengthening learning and capability building around our health and safety requirements, we also made it clear that failure to have controls in place will result in business consequences. As part of consequence management for 44 supplier related fatal, critical or high potential incidents that occurred during 2018, we issued 29 warning notes to our suppliers and terminated business relationships with 2 suppliers. Of the total 31 cases 84 percent were “high potential” where no one was critically or fatally injured. The consequence management committee does not issue cards based on severity but rather considers the control the supplier has in place when deciding on the consequence.
Combatting modern slavery in the supply chain

We do not tolerate slavery, servitude, trafficking in persons, and forced or compulsory labor in our own operations or in our supply chain.

In 2018 we published our second Modern Slavery statement, with an updated risk map. The statement can be found on our corporate website at www.nokia.com/about-us/sustainability/downloads.

Dealing with early warning signs

In 2018, as a result of our audits we encountered seven cases where we saw potential risk of forced labor and therefore classified it accordingly. Two of the cases were related to an obligation on employees to pay back course fees if they were to leave the company within six months after the training, which could place the employee at risk of being kept in a situation resulting in being forced to continue working as a result of not having the money to pay back the training fee. In another instance found in India, the supplier had not provided employees with appointment letters detailing relevant terms and conditions of employment. In another three cases, the percentage of dispatched workers exceeded the allowed 10 percent limit. And the last case was related to missing policy on forced labor.

Corporate responsibility risk map of our suppliers

This map is an aggregate of a selection of Verisk Maplecroft indices. The map covers countries where we have business with suppliers (exceeding a set minimum € threshold), but may not cover all countries where our suppliers operate. This was created based on Verisk Maplecroft’s Global Risks Portfolio.
These cases have been addressed with the suppliers as part of audit follow-up and the learnings have been shared with all of the suppliers at the supplier workshops in each location.

Child labor – zero tolerance
We have a strict policy against the use of child labor and we continuously work closely with our suppliers to scrutinize, monitor, and remediate any and all potential risks. We have strict ethical and human resources policies which have been designed to ensure that no one below the legal working age is hired in our business. If a child labor risk is identified, we immediately put in place a Child Labor Remediation Plan in line with SA8000 recommendations. In 2018, we encountered 3 findings at one of our audits related to a young worker who was working in a hazardous area (dust) and exposed to overtime. The factory also did not have the required registration approval for employment of young workers from the local labor bureau.

We further reiterated zero tolerance on the subject at all audits and workshops with suppliers, strengthening the message on requirements to map the related risks and develop child labor mitigation and remediation plans for direct and indirect forms of child labor, as well as special protection required for young people and student labor if they are employed.

Freedom of association and collective bargaining
All employees have the right to form or join their own organizations and conduct collective bargaining. We expect our suppliers to uphold that right, without obstruction or discouragement. Where there may be legal restrictions in place, we find alternative means to enable both individuals and groups to raise concerns to management. As a rule, our corporate responsibility audits include a review of freedom of association as one component of employee-management communications.

In 2018, we again noted potential risks of non-conformities as part of onsite audits related to employee-management communication. These included such examples as missing anonymous feedback and complaint channels or records of worker union representative elections.

The role of ICT in tackling modern slavery
In June 2018, we published our second Modern Slavery statement, with updated information. We continued our collaborative work to investigate ways in which the technology we provide can be used to eradicate modern slavery. We realize the potential risks of traffickers and other criminal groups and individuals using technology to conduct their criminal activities. We also realize that only by working with other key stakeholders can we drive greater impact and encourage concrete solutions to tackling issues related to modern slavery on the fight against trafficking, forced labor or modern slavery.

In June 2018, as co-founders with BT and Microsoft, we announced the formation and goals of the Tech Against Trafficking initiative. This coalition of global technology companies, civil society organizations, and the UN have come together in a collaborative effort to further support the eradication of forced labor and human trafficking. The company members of Tech Against Trafficking believe that technology can and must play a major role in preventing and disrupting human trafficking and empowering survivors. In 2018, the group began working with anti-trafficking experts to identify and investigate opportunities to develop and scale promising technologies.

The group embarked on an ambitious project to understand and map the landscape of existing technology tools being used in the anti-trafficking sector. Over 200 anti-trafficking tools were identified, with the majority (approximately 69 percent) working to identify existing victims of human trafficking and address and manage the risk of child and forced labor in corporate supply chains. The initiative intends to publish an interactive map of technology tools currently used to combat trafficking across the globe with the goal of increasing collaboration and encouraging the use of innovative technology. For more information visit BSR website.

During 2018, we continued to advocate for greater dialog on the issue of modern slavery and human rights across industry and civil society, participating in a number of events in London and elsewhere in Europe and the US.
A key area of our work with our supply chain is the ongoing potential risks identified in the mining, extraction and trade of metals that provide key minerals in electronic components.

Risks include military conflict, human and labor rights violations and damaging impacts on the environment.

It is therefore paramount that we are able to trace the materials used in our products and ensure they are conflict-free. We recognize that there are many complex issues associated with conflict minerals*, but through our work in this area we aim to contribute to a long-term solution that ensures responsible and conflict-free sourcing via legitimate trade that brings sustainable improvements in those countries where the risks are greatest. We demand that our suppliers commit to sourcing these key materials from environmentally and socially responsible sources. We require our suppliers to show their commitment to only sourcing these materials, that either directly or indirectly contribute to conflict, from environmentally and socially responsible sources.

As part of our work to ensure conflict-free minerals we collaborate with our industry peers through the Responsible Minerals Initiative to improve the traceability of minerals and ensure responsible sourcing. Our due diligence approach is aligned with the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals.

In 2018, we again underscored the need for our suppliers to establish full traceability of smelters in our supply chain and achieved a 97 percent rate of suppliers meeting our requirement. Where a supplier did not meet our objective or had no corrective action plan in place, we recommended phasing out this supplier from our supplier pool. We again held two workshops on conflict minerals and cobalt sourcing in China, perhaps our most challenging market in this area. Ten audits covering conflict minerals due diligence were also carried out in China during 2018.

In 2018 as part of our ongoing work with the Responsible Minerals Assurance Program (RMAP) to identify and validate the smelters and refineries in our supply chain that are conflict-free or active in the validation process, we achieved an 84 percent validation level. A further 5 percent of smelters were identified where our due diligence efforts have demonstrated that the smelters can be reasonably considered as conflict-free, for example, due to

* Columbite-tantalite (coltan) (or its derivative tantalum), cassiterite (or its derivative tin), gold and wolframite (or its derivative tungsten).
We have continued our work with the Public-Private Alliance, further contributing to the development of in-region programs. In 2018, we also conducted mapping of cobalt in our components based on part material declarations. We addressed 48 relevant suppliers about Nokia requirements related to Cobalt and engaged them in exercising due diligence over cobalt supply chain by using the industry’s Cobalt Reporting Template. Cobalt was also included in the scope of our workshops in China. We will continue cobalt-related due diligence in 2019. For more information on our due diligence results, please refer to our conflict minerals report available at the end of May 2019.

In 2018 we also engaged with our procurement category streams by setting minimum expectations for performance level of Preferred and Allowed status suppliers documented in procurement category strategies. The performance of suppliers across our sustainability monitoring programs such as onsite audits, CDP, EcoVadis, Supplier Health and Safety Maturity Assessment as well as Conflict Minerals program contribute to our sustainability pillar which is one of the six pillars of our Supplier Performance Evaluation.
How companies protect customer, employee, or other sensitive data is one of the most significant issues facing our industry today, and its importance grows ever greater as we see the implementation of 5G, IoT and AI, with everything and everyone connected.

We have dedicated processes firmly in place to address this, focusing on technical protection, processes, and people.

Technical protection includes, for example, security incident event monitoring (SIEM) by our security operations center (SOC), access management, anti-malware operations, certificate management, log provisioning, network security services, security incident management, server provisioning, software whitelisting and vulnerability remediation.

Process-related controls include business-driven governance, security as part of global business processes, integrated enterprise risk management, active third-party management and a dedicated security program to respond to our customers’ security and privacy requirements. Our internal processes help to enforce the proper handling, storage, transmission, and destruction of sensitive or confidential information.

Our ongoing key programs to identify and protect critical data include:
- critical information protection program
- focused assessments
- nokia privacy program
- supply chain security program
- customer security requirements program
- common security controls program
- selected ISO 27001 certifications

People-related mitigation relies on active security culture management, enabling and supporting employee security work, and employment life cycle management. To drive this, we have an internal accreditation program with three tiers. Approximately 30,000 of our employees have already completed it. Our security culture program also provides other learning channels such as regular company-wide phishing testing, mandatory e-learning for all employees and targeted campaigns. Our top management tracks how many personal learning moments (engagements) our people on average have throughout the year. This includes in addition to our security accreditation program, phishing testing and e-learning other activities like participation to our roadshows, targeted briefings, breach management trainings and exercises, and other related presentations.

Our market research reveals that security is an ever-growing concern within the telecommunications industry. We are firmly dedicated to protecting next-generation networks from attacks and are seen as a leader in the provision of network security solutions. We hold annual Security Days and Nokia HackAthons.

For more information on the solutions we provide to our customers visit networks.nokia.com/solutions/security.

Our breach management process is followed in the event of a breach or attack. The plan focuses on three key elements:
1. detection and analysis
2. containment, eradication, and recovery
3. post incident activities

We run a response function that consists of three teams—Incident Response Teams (IRTs), the Major Event Team (MET) and the Crisis Management Team (CMT)—depending on the type of incident or crisis. Each team has well defined tasks, and teams carry out training on an annual basis. Teams consist of subject matter experts from all areas of the company. Regular training and internal and external testing on our breach management capability is provided. The testing includes annual internal tabletop exercises, as well as annual external outside-in simulated attacks.

As is the case for all international companies with internet-facing services, we face daily attack attempts. We actively and regularly validate our security throughout the year through:
- external and internal security audits
- group-wide external maturity assessment
- external and internal simulated attacks (red team tests)
- regular group wide phishing testing
- external information security risk rating service
- customer feedback

Our market research reveals that security is an ever-growing concern within the telecommunications industry. We are firmly dedicated to protecting next-generation networks from attacks and are seen as a leader in the provision of network security solutions. We hold annual Security Days and Nokia HackAthons.
• external and internal ISO 27001 audits for our Global Delivery Centers

All our employees and external contractors are required to take mandatory Information Security e-learning courses every two years. New hires must take an e-learning course when starting with Nokia and our security awareness and culture Key Performance Indicators (KPIs) are tracked on a monthly level.

In 2018, we achieved our target to secure our defined critical information ecosystems and closed 95 percent of the identified critical and high vulnerabilities identified in our assessments and audits. We are well on track to achieve our 2020 target to be recognized as an industry leader in security and privacy.

Getting privacy right

With the growing complexities provided by today’s technology and business environment, it is imperative that we lead and enable strategic and consistent management of privacy related risks, as well as ensuring we are in a position to make the most of all the opportunities ahead. With the arrival of 5G and IoT, in a world where everyone and everything are increasingly connected, cloud storage, big data, and other technology advances, getting privacy right is not only desirable – it is a necessity.

We have established a comprehensive company-wide privacy program that is based on relevant laws, best practices and standards. This program is supported by and aligned with corporate, business group and central functions level policies and processes. Our objective is to mitigate privacy risk in relation to the data we collect, process and store. Essential to this approach is observing the concept of data minimization, meaning we endeavor only to collect personal data that is necessary for the purpose for which they are collected and to retain such data for no longer than necessary.

We then implement appropriate controls to ensure that all personal data is only accessed by persons with a clear and justifiable need to know. Should a personal data breach occur, we have a formal process in place to manage and mitigate any related risk to data subjects. These processes also include mechanisms to communicate with supervisory authorities, should that be required. To drive and
maintain privacy awareness, we have designed and delivered a program of awareness training targeting high-risk groups as well as all Nokia employees through a mandatory e-learning module. Employee responsibilities towards privacy are also covered in our Code of Conduct.

Our privacy management model is set out in our Group-wide Privacy Management Policy and supported by Nokia Executive Leadership. The model provides clear privacy principles and a governance framework to implement sound privacy related practices across our businesses. We continue to strengthen our framework with supporting policy and procedures. Thanks to our programmatic approach, we remain in a position of strength to safeguard personal data entrusted to us. During 2018, we updated our privacy processes in readiness for the GDPR (General Data Protection Regulation) ensuring they remain fit for purpose. We also rolled out mandatory privacy awareness training for all employees reminding everyone of the importance of protecting data and how they each have a part to play in relation to that objective.

Compliance with the new General Data Protection Regulation (GDPR) and other privacy laws as well as commitments to customers, are enforced via our Privacy Principles and Requirements.

There were no substantiated complaints regarding breaches of customer data in 2018.