



IMPLEMENTATION GUIDELINES FOR THE PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY

Contents

1. Purpose of This Document
2. Responsible Company Decision Making
3. Freedom of Expression and Privacy
4. Multi-Stakeholder Collaboration
5. Governance, Accountability & Transparency

Annex A: Definitions

1. Purpose of this Document

- 1.1 The Principles on Freedom of Expression and Privacy (the “Principles”) provide direction and guidance to the Information and Communications Technology (“ICT”) industry and its stakeholders in protecting and advancing the enjoyment of these human rights globally.
- 1.2 These Implementation Guidelines provide further details on how participating companies will put the Principles into practice. The purpose of this document is to:
 - a. Describe a set of actions by which a company would demonstrate that it is implementing the Principles with improvements over time.
 - b. Provide companies with direction and guidance on how to implement the Principles.
- 1.3 Participating companies will implement the Principles using these Implementation Guidelines. As described in the accompanying Accountability, Policy and Learning Framework, each participating company will be assessed every two years by independent assessors on its progress implementing the Principles. The GNI Board of Directors will determine whether a company is making good faith efforts to implement the GNI Principles with improvement over time.

- 1.4 The effectiveness of these Implementation Guidelines will be reviewed and assessed by the GNI Board of Directors as GNI's experience in the implementation of the Principles grows. The review process will include:
- a. Removing, revising or adding guidelines as appropriate.
 - b. Considering the development of specific sections in the Implementation Guidelines that may be tailored to specific challenges and issues relevant to different parts of the ICT sector.

2. Responsible Company Decision Making

Governance, Oversight and Leadership

- 2.1 The Board of Directors of a participating company is responsible for the strategic oversight of the company's human rights practices, including with respect to all company activities and operations affecting freedom of expression and privacy.

***Application Guidance:** A standing committee of the Board or subset of the entire Board may help the full Board of Directors in fulfilling its board responsibilities of strategic oversight. Where companies are subject to a two-tier board structure, the definition of the Board of Directors includes the "Executive Board", sometimes also called "Management Board".*

- 2.2 The Board will receive and evaluate regular human rights reporting from management including on how the commitments laid out in the Principles are being implemented.

***Application Guidance:** The Board may assign responsibility for addressing freedom of expression and privacy risks to senior level management with appropriate functions, within the company.*

- 2.3 The Board or Senior Management will:
- a. Review freedom of expression and privacy risks related to the company's operations in a manner consistent with the company's overall approach to risk management.

***Application Guidance:** freedom of expression and privacy risks refer to risks to individuals, including in unparticularized groups or communities, throughout this document.*

-
- b. Carry out the company's implementation of the Principles in a manner consistent with the safety and liberty of company personnel, including both employees and other persons working for a participating company.
 - c. Participate in appropriate freedom of expression and privacy risk training.

Application Guidance: *To ensure that training is meaningful and relevant, participating companies should take into account, the role and responsibilities of the Board member and / or senior management recipients when designing and implementing the training.*

- d. Establish clear instructions for when and how issues or problems affecting freedom of expression and privacy must be escalated to higher levels of the company.

Risk Management, Human Rights Impact Assessments and other Human Rights Due Diligence processes related to Freedom of Expression and Privacy

- 2.4 Consistent with the UN Guiding Principles on Business and Human rights, and considering international human rights standards, participating companies will carry out human rights due diligence to identify, prevent, evaluate, mitigate and account for risks to the freedom of expression and privacy rights that are implicated by the company's products, services, activities and operations. The process includes assessing actual and potential human rights impacts on individuals, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed as set forth in this section 2 of the Implementation Guidelines. In assessing actual and potential human rights impacts, companies should draw on a range of sources, including voices from inside relevant countries, human rights groups, government bodies, and international organizations. Companies should also evaluate whether relevant local laws and practices are consistent with rule of law requirements and international and regional human rights norms.
- 2.5 Human rights impact assessments and other due diligence processes should be ongoing, recognizing that the nature of the issues concerning freedom of expression and privacy may change over time as the company's operations and operating context evolve and as the human rights landscape changes in any particular jurisdiction.
- 2.6 If human rights due diligence as described in Section 2.4 above identifies circumstances when freedom of expression and privacy may be jeopardized or advanced, participating companies will employ human rights impact assessments and develop effective risk mitigation strategies as appropriate. The following are situations where human rights due diligence has revealed the need for human rights impact assessments:

- a. Reviewing and revising internal procedures for responding to government demands for user data or content restrictions in existing markets.
- b. Entering new markets, particularly those where freedom of expression and privacy are not well protected.
- c. Leaving markets, particularly those where freedom of expression and privacy are not well protected.
- d. Reviewing the policies, procedures and activities of potential partners, investments suppliers and other relevant related parties for protecting freedom of expression and privacy as part of its corporate due diligence process.
- e. Designing and introducing new technologies, products and services and their use.
- f. Acquiring other companies or forming operational partnerships (e.g., joint ventures).

2.7 The human rights impact assessments should be initiated early enough to inform the development of a new activity or relationship. They will be undertaken to different levels of detail and scope depending on the purpose of the impact assessment. However, participating companies should:

- a. Prioritize the use of human rights impact assessments for markets, business partners and other relationships, technologies (products / services) where the risk of adverse human rights impacts to freedom of expression and privacy is most salient or where the potential to advance human rights is at its greatest.
- b. Draw upon inputs from a variety of sources, including, for example, voices from inside the geography in question, human rights groups, government bodies, international organizations and materials developed as part of this multi-stakeholder process.
- c. Review the human rights risks and effects of not having operational control before entering or exiting joint ventures.
- d. Include a review of relevant domestic laws, legal systems and practices in each market and evaluate their conformity to rule of law requirements and international and regional human rights norms especially articles 19 and 12 of the

Universal Declaration of Human Rights and articles 19 and 17 of the International Covenant on Civil and Political Rights.

Application Guidance: *Regional human rights norms refer to the norms included in the African Charter on Human and People’s Rights, the American Convention on Human Rights, and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Since there may be inconsistencies and gaps between the protections afforded by various human rights instruments, the individual should be entitled to the most protective provisions of applicable law.*

- e. Utilize learning from real-life cases and precedents.
- f. Update human rights impact assessments over time, such as when there are material changes to laws, regulations, markets, products, technologies, or services.
- g. Take appropriate action to avoid, mitigate or in other ways address potential negative human rights impacts on an ongoing basis. For example, in order to prevent and mitigate adverse human rights impacts, participating companies will incorporate the findings from human rights impact assessments into other company processes and practices for risk review and risk management, including those carried out in connection with a merger or acquisition.
- h. Develop internal processes and mechanisms for using the results of impact assessments to inform company policy and practice.
- i. Demonstrate to external stakeholders consulted in the course of risk assessments that the findings are considered by senior management.

Partners, Suppliers and Distributors

2.8 Participating companies will follow these Principles and Implementation Guidelines in all circumstances when they have operational control.

Application Guidance: *“Operational control” means the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.*

2.9 When the participating company does not have operational control, it will use Best Efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow the Principles.

Application Guidance: *It is recognized that the influence of participating companies will vary across different relationships and contractual arrangements. “Best Efforts” means that the participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.*

- 2.10 With regards to third party relationships, participating companies should focus their efforts on those business partners, investments, suppliers, distributors and other relevant related parties that are involved in the participating company’s business in a manner that materially affects the company’s role in respecting and protecting freedom of expression and privacy. In doing so, the participating company should prioritize efforts on circumstances where the risks to freedom of expression and privacy are most salient.
- 2.11 Where participating companies may initially lack influence to prevent or mitigate adverse impact of business relationships, they should assess how they could increase their ability to address such adverse impacts over time.

Application Guidance: It is assumed that this approach will be taken in all relevant contracts signed after committing to the Principles and to all relevant pre-existing contracts

Integration into Business Operations

- 2.12 Participating companies will develop appropriate internal structures and take steps throughout their business operations to ensure that the commitments laid out in the Principles are incorporated into company analysis, decision making and operations.
- 2.13 Over time this will include:

Structure

- a. The creation of a senior-directed, human rights function, including the active participation of senior management, to design, coordinate and lead the implementation of the Principles.

Application Guidance: *This function may be organized differently within companies; it may consist of a dedicated human rights team or the function may build on new or existing internal corporate structures, such as sustainability / corporate social responsibility, policy, privacy or compliance /business ethics roles or (virtual and / or cross-functional) teams.*

- b. Ensuring that the procedures related to government demands implicating users’ freedom of expression or privacy rights are overseen and signed-off by an

appropriate and sufficiently senior member of the company's management and are appropriately documented.

Procedures

- c. Establishing written procedures that ensure consistent implementation of policies that protect freedom of expression and privacy and documenting implementation of these policies. Documentation of policies and their implementation should be sufficiently detailed as to enable later internal and external review.
- d. Incorporating freedom of expression and privacy review into assurance processes to ensure implementation of the procedures laid out in the Principles.
- e. Maintaining a record of requests and demands for government restrictions to freedom of expression and access to personal information.

Remedy / Grievance

- f. Establishing grievance mechanisms for users to make it possible for grievances about issues related to freedom of expression and privacy to be communicated to the company for consideration and, if appropriate, direct remediation. If a participating company determines its business practices are inconsistent with the Principles or have caused or contributed to adverse impacts, it will establish by itself or in cooperation with other actors, a means of remediation, including meaningful steps to prevent recurrence of such inconsistency or impact.

Application Guidance: to ensure their effectiveness, the grievance mechanisms should be designed in accordance with the effectiveness criteria set out in principle 31 of the UN Guiding Principles on Business and Human Rights.

- g. Providing whistleblowing mechanisms or other secure channels through which employees can confidentially or anonymously report violations of the Principles without fear of associated punishment or retribution.

Application Guidance: For example, each company might appoint or designate an internal ombudsman, auditor or compliance officer to monitor the company's business practices which includes issues relating to freedom of expression and privacy.

Employees

- h. Communicating the Principles and / or company policies that implement the Principles to all relevant employees through internal channels, such as through the company intranet, and integrate the company's commitment to the Principles through employee training or orientation programs.

- i. Providing more detailed training for those corporate employees who are most likely to face freedom of expression and privacy challenges, based on human rights impact assessments. This may include staff in audit, compliance, legal, marketing, sales and business development areas. Where appropriate and feasible, the orientation and training programs should also be provided to employees of relevant related parties such as partners, suppliers and distributors.
- j. Developing escalation procedures for employees seeking guidance in implementing the Principles.

3. Freedom of Expression and Privacy

Government Demands, Laws and Regulations

3.1 Participating companies will:

- a. Encourage governments to be specific, transparent and consistent in the demands, laws and regulations (“government restrictions and demands”) that impact freedom of expression or the right to privacy, including e.g. restrictions of access to content or restrictions of communications, or demands that are issued regarding privacy in communications.
- b. Encourage government restrictions and demands that are consistent with international laws and standards on freedom of expression and privacy. This includes engaging proactively with governments to reach a shared understanding of how government restrictions can be applied in a manner consistent with the Principles.
- c. Adopt policies and procedures which set out how the company will assess and respond to government demands for restrictions to communications or access to content, or disclosure of personal information.
- d. These policies and procedures will also address how the company will respond in instances when governments fail to provide a written directive or adhere to domestic legal procedure. They will also include a consideration of when to challenge such government restrictions and demands.

Application Guidance: *Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*

3.2 When required to restrict communications, or remove content, or to provide personal information to government authorities, participating companies will:

- a. Require that governments follow established domestic legal processes when they are seeking to (1) restrict freedom of expression or (2) access personal information.
- b. Request clear written communications from the government that explain the legal basis for government restrictions to freedom of expression and government demands for personal information, including the name of the requesting government entity and the name, title and signature of the authorized official.

Application Guidance: *Written demands are preferable, although it is recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.*

- c. Keep - where the law permits verbal demands and in emergency situations, when communications will be oral rather than written - records of these demands.
- d. Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression.
- e. Narrowly interpret and implement government demands that compromise privacy.
- f. Narrowly interpret the governmental authority's jurisdiction so as to minimize the negative effect on freedom of expression.
- g. Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that country.

Application Guidance: *It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*

3.3 When faced with a government restriction or demand that appears overbroad, unlawful, or otherwise inconsistent with domestic laws or procedures or international human rights

laws and standards on freedom of expression or privacy, participating companies will in appropriate cases and circumstances:

- a. Seek clarification or modification from authorized officials of such requests;
- b. Seek the assistance, as needed, of relevant government authorities, international human rights bodies or non-governmental organizations; and
- c. Challenge the government in domestic courts.

Application Guidance: *Overbroad could mean, for example, where more information is restricted than would be reasonably expected based on the asserted purpose of the request.*

Application Guidance: *It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression and privacy, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.*

Data Collection

3.4 Participating companies will assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate and develop appropriate mitigation strategies to address these risks.

Communications with Users and the Public

Participating companies will seek to operate in a transparent manner when required by government to restrict communications or access to content or provide personal information to governments. To achieve this, participating companies will:

- a. Disclose to users in clear language the generally applicable laws and policies which require the participating company to remove or limit access to content or restrict communications or provide personal information to government authorities.
- b. Disclose to users in a clear manner the company's policies and procedures for responding to government restrictions and demands to remove or limit access to content, restrict communications or provide personal data.

-
- c. Give clear, prominent and timely notice to users when access to specific content has been removed or blocked by the participating company or when communications have been limited or stopped by the participating company due to government restrictions. Notice should include the reason for the action and state on whose authority the action was taken.
 - d. Disclose to users in clear language what personal information the participating company collects, and the participating company's policies and procedures for responding to government demands for personal information.
 - e. Assess on an ongoing basis measures to effectively support transparency with users, regarding the company's data collection, storage, and retention practices.

4. Multi-Stakeholder Collaboration

Engagement in Public Policy

- 4.1 Participants will individually and collectively, through GNI or otherwise, encourage governments and international institutions to adopt policies, practices and actions that are consistent with and advance the Principles.
- 4.2 Participants will:
 - a. Engage government officials to promote rule of law, transparency, the principles of legality, necessity and proportionality as well as the reform of laws, policies and practices that infringe on freedom of expression and privacy.

***Application Guidance:** Promoting rule of law reform could include rule of law training, capacity building with law-related institutions, taking public policy positions or external education.*

- b. Engage in discussions with home governments to promote understanding of the Principles and to support their implementation
- c. Encourage direct government-to-government contacts to support such understanding and implementation.
- d. Encourage governments, international organizations and entities to call attention to the worst cases of infringement on the human rights of freedom of expression and privacy.

- e. Acknowledge and recognize the importance of initiatives, that seek to identify, prevent and limit access to illegal online activity such as child exploitation. The Principles and Implementation Guidelines do not seek to alter participants' involvement in such initiatives.
- f. Participants will refrain from entering into voluntary agreements that require the participants to limit users' freedom of expression or privacy in a manner inconsistent with the Principles. Voluntary agreements entered into prior to committing to the Principles and which meet this criterion should be revoked within three years of committing to the Principles.

Application Guidance: *It is recognized that participants may take different positions on specific public policy proposals or strategies, so long as they are consistent with the Principles.*

Internal Advisory Forum

- 4.3 A confidential multi-stakeholder Advisory Forum within the GNI will provide guidance to participating companies on emerging challenges and opportunities to respect and advance the human rights of freedom of expression and privacy.

External Multi-Stakeholder Learning Forums

- 4.4 Participants will promote global dialogue and understanding of the Principles and share learning about their implementation. Participants will engage with a broad range of interested companies, industry associations, advocacy NGOs and other civil society organizations, universities, governments and international institutions.
- 4.5 Participants will create a global learning, collaboration and communication program. This program will identify stakeholders, topics and forums for learning, collaboration and communication activities.

Application Guidance: *This could include, for example, the Internet Governance Forum, the International Telecommunications Union, the UN Special Procedures, the UN Global Compact, the Council of Europe, and the Freedom Online Coalition.*

- 4.6 Part of the GNI learning program will be an annual Multi-stakeholder Learning Forum focusing on the rights to freedom of expression and privacy, the specific scenarios in which these rights are affected and other broader issues related to the implementation of the Principles.

- 4.7 Where participants have activities or operations in the same countries, territories, and regions they will seek to collaborate on the development of local dialogues on relevant prominent issues and emerging concerns in those localities.
- 4.8 Participants will develop and share tools, resources, processes and information that support the implementation of the Principles.
- 4.9 Included in the learning program will be a consideration of the role that tools such as encryption, anonymizing technologies, security enhancements and proxy technologies can play in enabling users to manage their media experiences and protect freedom of expression and privacy.

Governance, Accountability & Transparency

Governance

- 5.1 A multi-stakeholder representative Board will oversee this initiative, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Reporting on Implementation

- 5.2 There will be three different levels of reporting on the progress being made to implement the Principles, described in more detail in the accompanying Accountability, Policy and Learning Framework document.

Independent Assessment

- 5.3 There will be a system of independent assessment of the implementation of the Principles, described in more detail in the accompanying Accountability, Policy and Learning Framework document.

Transparency

- 5.4 Participating companies will communicate their general approach to addressing their human rights impacts in relation to freedom of expression and privacy (e.g. informal engagement with relevant stakeholders, public communications, formal public reporting). Participating companies will also communicate every two years to the public

about the outcome of their independent assessment, as described in the accompanying Accountability, Policy and Learning Framework document.

6. Annex A: Definitions

Freedom of Expression: Freedom of expression is defined using Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

ICCPR:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
 - (a) For respect of the rights or reputations of others;
 - (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

Privacy: Privacy is defined using Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ICCPR:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

Rule of Law: A system of transparent, predictable and accessible laws and independent legal institutions and processes, which respect, protect, promote and fulfil human rights.

Personal Information: Participants are aware of the range of definitions for “personal information” or “personally identifiable information” and acknowledge that these definitions vary between jurisdictions. These Implementation Guidelines use the term “personal information” and interpret this to mean information that can, alone or in aggregate, be used to identify or locate an individual (such as name, email address or billing information) or information which can be reasonably linked, directly or indirectly, with other information to identify or locate an individual.

User: Any individual using a publicly available electronic communications service, for private or business purposes, with or without having subscribed to this service.

Best Efforts: The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion