

Global Network Initiative

*Protecting and Advancing Freedom of Expression and Privacy
in Information and Communications Technologies*

Implementation Guidelines for the Principles on Freedom of Expression and Privacy

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

Annex A: Definitions

1. Purpose of this Document

The Principles on Freedom of Expression and Privacy (the “Principles”) have been created to 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.

These Implementation Guidelines provide further details on how participating companies will put the Principles into practice. The purpose of this document is to:

- Describe a set of actions which constitute compliance with the Principles.
- Provide companies with guidance on how to implement the Principles.

As described in the accompanying Governance, Accountability and Learning Framework, each participating company will be assessed on their progress implementing the Principles after two years and annually thereafter.

The effectiveness of these Implementation Guidelines will be reviewed and assessed as experience in implementation of the Principles grows. The review process will include:

- Removing, revising or adding guidelines as appropriate.
- Considering the development of different versions of the Implementation Guidelines that may be tailored to specific regions or sectors.

2. Responsible Company Decision Making

Board Review, Oversight and Leadership

The Boards of participating companies will incorporate the impact of company operations on freedom of expression and privacy into the Board’s review of the business.

The Board will:

- Receive and evaluate regular reports from management on how the commitments laid out in the Principles are being implemented.
- Review freedom of expression and privacy risk within the overall risk management review process.
- Participate in freedom of expression and privacy risk training as part of overall Board education.

Application Guidance: “Board” could mean a Management Board or Executive Board if these are more appropriate for the participating company’s structure.

Human Rights Impact Assessments

Participating companies will employ human rights impact assessments to identify circumstances when freedom of expression and privacy may be jeopardized or advanced, and develop appropriate risk mitigation strategies when:

- Reviewing and revising internal procedures for responding to government demands for user data or content restrictions in existing markets
- Entering new markets, particularly those where freedom of expression and privacy are not well protected.
- 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.
- Designing and introducing new technologies, products and services.

The human rights impact assessments will be undertaken to different levels of detail and scope depending on the purpose of the impact assessment. However, participating companies should:

- Prioritize the use of human rights impact assessments for markets, products, technologies and services that present the greatest risk to freedom of expression and privacy or where the potential to advance human rights is at its greatest.
- Update human rights impact assessments over time, such as when there are material changes to laws, regulations, markets, products, technologies, or services.
- Draw upon resources from human rights groups, government bodies, international organizations and materials developed as part of this multi-stakeholder process.
- Include a consideration of relevant local laws in each market and whether the domestic legal systems conform to rule of law requirements.
- Utilize learning from real life cases and precedents.
- Focus on potential partners, investments, suppliers 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 privacy and freedom of expression.

- Incorporate the outputs of human rights impact assessments into other company processes, such as corporate risk assessments and due diligence.

Partners, Suppliers and Distributors

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

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.

Participating companies should focus their efforts on 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. The participating company should prioritize circumstances where it has the greatest influence and/or where the risk to freedom of expression and privacy is at its greatest.

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.*

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.*

Application Guidance: *It is recognized that the influence of participating companies will vary across different relationships and contractual arrangements. See the definition of "best efforts" provided in Annex A.*

Integration into Business Operations

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.

Over time this will include:

Structure

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

Application Guidance: *This team may build on existing internal corporate structures, such as corporate social responsibility, policy, privacy or business ethics teams.*

- 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

- Establishing written procedures that ensure consistent implementation of policies that protect freedom of expression and privacy and documenting compliance with these

policies. Documentation of policies and compliance should be sufficiently detailed as to enable later internal and external review.

- Establishing a means of remediation when business practices that are inconsistent with the Principles are identified, including meaningful steps to ensure that such inconsistencies do not recur.
- Incorporating freedom of expression and privacy compliance into assurance processes to ensure compliance with the procedures laid out in the Principles.
- Maintaining a record of requests and demands for government restrictions to freedom of expression and access to personal information.

Employees

- Communicating the Principles to all employees, such as through the company intranet, and integrating the company's commitment to the Principles through employee training or orientation programs.
- 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.

Complaints and Assistance

- Developing escalation procedures for employees seeking guidance in implementing the Principles.
- Providing whistle-blowing mechanisms or other secure channels through which employees and other stakeholders can confidentially or anonymously report violations of the Principles without fear of associated punishment or retribution.

Note: For example, each company might appoint or designate an internal ombudsman or auditor to monitor the company's business practices relating to freedom of expression and privacy.

3. Freedom of Expression

Government Demands, Laws and Regulations

Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government restrictions") that are issued to restrict freedom of expression online.

Participants will also encourage government demands that are consistent with international laws and standards on freedom of expression. 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.

When required to restrict communications or remove content, participating companies will:

- Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression.
- Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression.
- Interpret the governmental authority's jurisdiction so as to minimize the negative effect on to freedom of expression.

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.*

- Seek clarification or modification from authorized officials when government restrictions appear overbroad, not required by domestic law or appear inconsistent with international human rights laws and standards on freedom of expression.

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.*

- Request clear written communications from the government that explain the legal basis for government restrictions to freedom of expression, 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.*

- Adopt policies and procedures to address how the company will respond in instances when governments fail to provide a written directive or adhere to domestic legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- Challenge the government in domestic courts or seek the assistance of relevant government authorities, international human rights bodies or non-governmental organizations when faced with a government restriction that appears inconsistent with domestic law or procedures or international human rights laws and standards on freedom of expression

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, 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.*

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.*

Communications With Users

Participating companies will seek to operate in a transparent manner when required by government to remove content or otherwise limit access to information and ideas. To achieve this, participating companies will, unless prohibited by law:

- Clearly disclose to users the generally applicable laws and policies which require the participating company to remove or limit access to content or restrict communications.
- Disclose to users in a clear manner the company's policies and procedures for responding to government demands to remove or limit access to content or restrict communications.
- 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 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.

4. Privacy

Data Collection

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

Government Demands, Laws and Regulations

Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government demands") that are issued regarding privacy online.

Participating companies will also encourage government demands that are consistent with international laws and standards on privacy. This includes engaging proactively with governments to reach a shared understanding of how government demands can be issued and implemented in a manner consistent with the Principles.

Participating companies will adopt policies and procedures which set out how the company will assess and respond to government demands for disclosure of personal information. When required to provide personal information to governmental authorities, participating companies will:

- Narrowly interpret and implement government demands that compromise privacy.
- Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy.

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

- Request clear communications, preferably in writing, that explains the legal basis for 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.*

- Require that governments follow established domestic legal processes when they are seeking access to personal information.
- Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- 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.*

- Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.

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 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.*

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.*

Communications with Users

Participating companies will seek to operate in a transparent manner when required to provide personal information to governments. To achieve this, participating companies will:

- Disclose to users in clear language what generally applicable government laws and policies require the participating company to provide personal information to government authorities, unless such disclosure is unlawful.
- 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.
- Assess on an ongoing basis measures to support user transparency, in an effective manner, regarding the company's data collection, storage, and retention practices.

Application Guidance: *Participating companies will work with the Organization to raise awareness among users regarding their choices for protecting the privacy of their personal information and the importance of company data practices in making those choices.*

5. Multi-stakeholder Collaboration

Engagement in Public Policy

Participants will encourage governments and international institutions to adopt policies, practices and actions that are consistent with and advance the Principles.

Individually or collectively participants will:

- Engage government officials to promote rule of law and 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.

- Engage in discussions with home governments to promote understanding of the Principles and to support their implementation.
- Encourage direct government-to-government contacts to support such understanding and implementation.
- 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.
- 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.

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 these principles.

Internal Advisory Forum

A confidential multi-stakeholder Advisory Forum will provide guidance to participating companies on emerging challenges and opportunities for the advancement of freedom of expression and privacy.

External Multi-stakeholder Learning Forums

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.

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 Global Compact and the UN Special Representative of the Secretary General on human rights and transnational corporations and other business enterprises.

Part of this 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.

Where participants have activities or operations in the same countries they will seek to collaborate on the development of local dialogues on relevant prominent issues and emerging concerns in those localities.

Participants will develop and share innovative tools, resources, processes and information that support the implementation of the Principles.

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.

6. Governance, Accountability and Transparency

Governance

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

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

Independent Assessment

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

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 fulfill 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.