INTERNATIONAL STANDARDS

The legal and regulatory framework plays an important role in protecting human rights within the ICT sector. Here are some of the main binding and non-binding international instruments and standards, and relevant regulatory developments.

1. INTERNATIONAL STANDARDS / INSTRUMENTS

ORGANIZATION	NAME	OBJECTIVE	RELEVANT CONTENT
World Intellectual Property Organization	Convention Establishing the World Intellectual Property Organization -WIPO (1979)	WIPO's two main objectives are (i) to promote the protection of intellectual property worldwide; and (ii) to ensure administrative cooperation among the intellectual property Unions established by the treaties that WIPO administers.	Signed at Stockholm on July 14, 1967, entered into force in 1970 and was amended in 1979. WIPO is an intergovernmental organization which in 1974 became one of the specialized agencies of the United Nations system. The origins of WIPO go back to 1883 and 1886 when the Paris Convention for the Protection of Industrial Property and the Berne Convention for the Protection of Literary and Artistic Works provided for the establishment of an "International Bureau". The two bureaus were united in 1893 and, in 1970, were replaced by the World Intellectual Property Organization, by virtue of the WIPO Convention.
OECD	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)	These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of	OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such

		their nature or the context in which they are used, pose a danger to privacy and individual liberties.	human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it. The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23 September 1980. The Guidelines are accompanied by an Explanatory Memorandum intended to provide information on the discussion and reasoning underlining their formulation.
United Nations	The promotion, protection and enjoyment of human rights on the Internet - Resolution A/HRC/RES/20/8 (2012)	Recognizing the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms. Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in	Calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries. Encourages the special procedures to take these issues into account within their existing

		accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;	mandates, as applicable; Decides to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies, as well as of how the Internet can be an important tool for development and for exercising human rights, in accordance with its programme of work.information and communications technologies
United Nations	The right to privacy in the digital age - General Assembly Resolution A/C.3/68/L.45/Rev.1 (2013)	Calls upon all States to: (a) respect and protect the right to privacy, including in the context of digital communication; (b) take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; (c) review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of	The resolution also requests the United Nations High Commissioner for Human Rights to present a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States.

		all their obligations under international human rights law; (d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data.	
United Nations	Convention on the Rights of the Child - General comment No. 16 on State obligations regarding the impact of the business sector on children's rights (2013)	The general comment addresses States to have adequate legal and institutional frameworks to respect, protect and fulfil children's rights, and to provide remedies in case of violations in the context of business activities and operations; but also addresses obligations regarding not-for-profit organizations that play a role in the provision of services that are critical to the enjoyment of children's rights.	Expressly details "State obligations regarding the impact of the business sector on children's rights." Excerpt: "…States should…coordinate with the information and communication technology industry so that it develops and puts in place adequate measures to protect children from violent and inappropriate material."
United Nations	The right to privacy in the digital age – Resolution A/RES/68/167 (2013)	Recognizes the global and open nature of the Internet and the rapid advancement in information and communication technologies as a driving force in accelerating progress towards development in its various forms.	Affirms that the same rights that people have offline must also be protected online, including the right to privacy (also relates to internet rights, specifically with respect to digital surveillance)
United Nations	Information and communications technologies for development – Resolution A/RES/68/198	Recognizes that information and communications technologies have the potential to provide new solutions to development challenges, particularly in the	the need for respect for national sovereignty and applicable international law in the consideration of information and

	(2013)	context of globalization, and can foster sustained, inclusive and equitable economic growth and sustainable development, competitiveness, access to information and knowledge, poverty eradication and social inclusion that will help to expedite the integration of all countries, especially developing countries, in particular the least developed countries, into the global economy	communications technologies for development, noting the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies, and reaffirming that the same rights people have offline must also be protected online, including the right to privacy, as set out in its resolution entitled "The right to privacy in the digital age".

2. REGIONAL STANDARDS / INSTRUMENTS

ORGANIZATION	NAME	OBJECTIVE	RELEVANT CONTENT
Inter-American Specialized Conference on Human Rights	American Convention on Human Rights (1969)	To consolidate in the hemisphere, within the framework of democratic institutions, a system of personal liberty and social justice based on respect for the essential rights of man. Chapter I establishes the general obligation of the states parties to uphold the rights set forth in the Convention to all persons under their jurisdiction, and to adapt their domestic laws to bring them into line with the Convention. The 23 articles of Chapter II give a list of individual civil and political rights due to all persons, including the right to life "in general, from the moment of conception" to	In the ensuing years, the states parties to the American Convention have supplemented its provisions with two additional protocols: - Convention on Human Rights in the area of Economic, Social, and Cultural Rights (more commonly known as the "Protocol of San Salvador"). - Protocol to the American Convention on Human Rights to Abolish the Death Penalty.

		humane treatment, to a fair trial, to privacy, to freedom of conscience, freedom of assembly, freedom of movement, etc.	
Council of Europe	The Council of Europe Convention 108 [re] Personal Data (1981)	The object of the Convention is to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them. There is a need for such legal rules in view of the increasing use made of computers for administrative purposes. Compared with manual files, automated files have a vastly superior storage capability and offer possibilities for a much wider variety of transactions, which they can perform at high speed. Further growth of automatic data processing in the administrative field was expected in the years ahead as a result of the lowering of data processing costs, the availability of "intelligent" data processing devices and the establishment of new telecommunication facilities for data transmission.	"Information power" brings with it a corresponding social responsibility of the data users in the private and public sector. In modern society, many decisions affecting individuals are based on information stored in computerized data files: payroll, social security records, medical files, etc. These files should not grant an undeniable advantage through automatic data processing and lead to a weakening of the position of the persons on whom data are stored. Therefore, good quality of information must be maintained and storage of information which is not necessary for the given purpose must be refrained. Those in charge of the data must also guard against unauthorized disclosure or misuse of the information, and protect the data, hardware and software against physical hazards.
Council of Europe	The Council of Europe	The Convention is the first international treaty on crimes committed via the	The following offences are defined by the Convention: illegal

	Convention 185 on Cybercrime (2001)	Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.	access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright and neighbouring rights. It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties. Further, as conditions and safeguards, the Convention requires the provision for adequate protection of human rights and liberties, including

			rights arising pursuant to obligations under European Convention on Human Rights, International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and shall incorporate the principle of proportionality.
European Union	EU General Data Protection Regulation (EU-GDPR) (2001)	Is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.	Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personal data of individuals (formally called data subjects in the GDPR) inside the European Union, and applies to an enterprise established in the EU or—regardless of its location and the data subjects' citizenship—that is processing the personal data of people inside the EU. Controllers of personal data must put in place appropriate technical and organisational measures to implement the data protection principles. "Data protection by design and by default", means that business processes that handle personal data must be designed and built with consideration of the

			principles and provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate), and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit, informed consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation or unless the data controller or processor has received an unambiguous and individualized affirmation of consent from the data subject. The data subject has the right to revoke this consent at any time.
Asia Pacific Economic Cooperation	APEC Privacy Framework (2005)	The Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines), and reaffirms the value of privacy to individuals and to the information society. The previous version of the Framework (2005) was	Ministers have endorsed the APEC Privacy Framework, recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region. The APEC Privacy Framework promotes a

		modelled upon the OECD Guidelines (1980) which at that time represented the international consensus on what constitutes fair and trustworthy treatment of personal information. The updated Framework (2015) draws upon concepts introduced into the OECD Guidelines (2013) with due consideration for the different legal features and context of the APEC region.	flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.
African Union	African Union Convention on Cyber Security and Personal Data Protection (2014)	The goal of this Convention is to address the need for harmonized legislation in the area of cyber security in Member States of the African Union, and to establish in each State party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use; that by proposing a type of institutional basis, the Convention guarantees that whatever form of processing is used shall respect the basic freedoms and rights of individuals while also taking into account the prerogatives of States, the rights of local communities and the interests of businesses; and take on board internationally recognized best practices;	The Convention seeks, in terms of substantive criminal law, to modernize instruments for the repression of cybercrime by formulating a policy for the adoption of new offences specific to ICTs, and aligning certain offences, sanctions and criminal liability systems in force in Member States with the ICT environment.

3. OTHER NON-BINDING INSTRUMENTS AND INITIATIVES

ORGANIZATION	NAME	OBJECTIVE	RELEVANT CONTENT
United Nations	UN Guiding Principles on Business and Human Rights (2011)	Adopted by consensus by the governments on the UN Human Rights Council in 2011, these Principles cover three "pillars": The State Duty to Protect; The Corporate Responsibility to Respect; and Access to Remedy.	
OECD	OECD Council Recommendation on Principles for Internet Policy Making (2011)	Provides context and support to Members and stakeholders in their effort to implement effective and compatible approaches for Internet policy making, both at the national and international levels.	Recommends that, in developing or revising their policies for the Internet Economy, Members, in co-operation with all stakeholders, take account of the following high level principles as: 1. Promote and protect the global free flow of information; 2. Promote the open, distributed and interconnected nature of the Internet; 3. Promote investment and competition in high speed networks and services; 4. Promote and enable the cross-border delivery of services; 5. Encourage multi-stakeholder co-operation in policy development processes; 6. Foster voluntarily developed codes of conduct; 7. Develop capacities to bring publicly available,

			reliable data into the policy-making process; 8. Ensure transparency, fair process, and accountability; 9. Strengthen consistency and effectiveness in privacy protection at a global level; 10. Maximise individual empowerment; 11. Promote creativity and innovation; 12. Limit Internet intermediary liability; 13. Encourage co-operation to promote Internet security; 14. Give appropriate priority to enforcement efforts.
Global Network Initiative	GNI Principles (Principles on Freedom of Expression and Privacy) 2017	The GNI Principles have been developed by companies, investors, civil society organizations and academics (collectively "the participants") who aim to protect and advance freedom of expression and privacy in the Information and Communications Technology (ICT) industry globally.	GNI Principles are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR"). The application of these Principles is informed by the UN Guiding Principles on Business and Human Rights ("UN Guiding Principles"), the 'Protect, Respect, and Remedy' Framework, and the OECD

			Guidelines for Multinational Enterprises.
Privacy organizations and advocates worldwide, including but not limited to Access, Article 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India, Comisión Colombiana de Juristas,Electronic Frontier Foundation, European Digital Rights, Fundación Karisma, Open Net Korea, Open Rights Group, Privacy International, and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic	International Principles on the Application of Human Rights to Communications Surveillance (2014)	Clarify how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to Communications Surveillance technologies and techniques.	With over 450 signatories from civil society and academia, these principles can provide civil society groups, industry, States, and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights. Are the outcome of a global consultation with civil society groups, industry, and international experts in Communications Surveillance law, policy, and technology.