Mapping of the Respect Principles to Fair Information Practices Principles

VERSION 2.1 – 2016-02-01

Abstract

This subdocument of the Respect Trust Framework™ provides a mapping between the Respect Principles and Fair Information Practices Principles (FIPPs) as defined by different governing bodies around the world.

Table of Contents

Comparison Table

This table provides a comparison of the five Respect Principles in the Respect Trust Framework with Fair Information Practices Principles from around the world.

Duty on Member	Right	Canada	Sweden	COP (Great Britain)	EU	EU	NSTIC	COE
					EU - 95/46/EC	EU-2002/58/EC		
Respect other Members' input and output controls	Identity Integrity	C-3 C-4 C-6 C-9	SW-1 SW-5 SW-6 SW-7 SW-8 SW-9	COP-1 COP-3 COP-4 COP-5 COP-8 COP-9 COP-10	EU 95-1 EU 95-3 EU 95-4 EU 95-5	EU 02-1 EU 02-2 EU 02-3 EU 02-4 EU 02-5 EU 02-6 EU 02-7	N-1 N-4	COE-1 COE-2 COE-3 COE-4 COE-5 COE-6 COE-9 COE-10
Ask permission before using or sending data/identity, Honest Dealing	Negotiation	C-2 C-3 C-5	SW-3 SW-4	COP-1 COP-2	EU 95-2	EU 02-2 EU 02-3 EU 02-4 EU 02-5 EU 02-6 EU 02-7	N-2 N-3 N-5 N-6	COE-2 COE-8 COE-11
Protect data/identity in possession from third parties	Safety from third party access	C-7	SW-9	COP-6 COP-7 COP-8	EU 95-5	EU 02-1 EU 02-3	N-4 N-7	COE-5 COE-6 COE-7
Allow data subject access and use of data/identity held about them	Freedom of movement	C-9						COE-9
Information sharing, cooperation	Fair systems information access, knowledge	C-1 C-8 C-9 C-10	SW-7	COP-9		EU 02-6	N-1 N-6 N-8	

Duty on Member	Right	OECD	HEW-1	PPSC	FTC	OITF	DHS	APEC	GSMA
Respect other Members' input and output controls	Identity Integrity	OECD-1 OECD-2 OECD-3 OECD-6	HEW-1 HEW-2 HEW-4 HEW-5	PPSC-1 PPSC-2 PPSC-3 PPSC-4 PPSC-5 PPSC-6 PPSC-7	FTC-3 FTC-4	OITF-1 OITF-3 OITF-4 OITF-7	DHS-2 DHS-3 DHS-4 DHS-6 DHS-7	A-1 A-2 A-3 A-4 A-6 A-8	GSMA-1 GSMA-2 GSMA-4 GSMA-8
Ask permission before using or sending data/identity, Honest Dealing	Negotiation	OECD-1 OECD-3 OECD-4 OECD-7	HEW-3	PPSC-4 PPSC-6 PPSC-8	FTC-1 FTC-2	OITF-7	DHS-2 DHS-6 DHS-8	A-2 A-3 A-4 A-5 A-9	GSMA-1 GSMA-2 GSMA-3 GSMA-5 GSMA-7
Protect data/identity in possession from third parties	Safety from third party access	OECD-5	HEW-5	PPSC-7 PPSC-8	FTC-4	OITF-9	DHS-5	A-1 A-7 A-9	GSMA-4 GSMA-6 GSMA-8
Allow data subject access and use of data/identity held about them	Freedom of movement	OECD-7		PPSC-2		OITF-6		A-8	GSMA-5
Information sharing, cooperation	Fair systems information access, knowledge	OECD-6 OECD-7 OECD-8		PPSC-1 PPSC-2 PPSC-8	FTC-3	OITF-2 OITF-4 OITF-8 OITF-10 OITF-11 OITF-12	DHS-1	A-2 A-9	GSMA-1 GSMA-9

Table of the Respect Principles

RESPECT TRUST FRAMEWORK	
R-1	**PROMISE:** Every Member promises to respect the right of every other Member to control the Member Information they share within the network and the communications they receive within the network.
R-2	**PERMISSION:** As part of this promise, every Member agrees that all sharing of Member Information and sending of communications will be by permission, and to be honest, direct and fair about the purpose(s) for which permission is sought.
R-3	**PROTECTION:** As part of this promise, every Member agrees to provide reasonable protection for the privacy and security of Member Information shared with that Member.
R-4	**PORTABILITY:** As part of this promise, every Member agrees that if it hosts Member Information on behalf of another Member, the right to possess, access, control, and share the hosted information, including the right to move it to another host, belongs to the hosted Member.
R-5	**PROOF:** As part of this promise, every Member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.

Canada

CANADA	
C-1	**ACCOUNTABILITY:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
C-2	**IDENTIFYING PURPOSES:** The purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.
C-3	**CONSENT:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
C-4	**LIMITING COLLECTION:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
C-5	**LIMITING USE, DISCLOSURE, AND RETENTION:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
C-6	**ACCURACY:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
C-7	**SAFEGUARDS:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
C-8	**OPENNESS:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
C-9	**INDIVIDUAL ACCESS:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended.
C-10	**CHALLENGING**: Compliance an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Sweden

SWEDEN	
SW-1	The controller shall, inter alias, ensure that personal data is only processed if it is lawful.
SW-2	The controller shall, inter alia, ensure that personal data is processed in a proper manner and in accordance
SW-3	The controller shall, inter alia, ensure that personal data is gathered only for specific, explicitly stated and legitimate purposes.
SW-4	The controller shall, inter alia, ensure that personal data is not processed for any purpose that is incompatible with that for which the data was gathered.
SW-5	The controller shall, inter alia, ensure that personal data that is treated is adequate and relevant to the purpose of the processing.
SW-6	The controller shall, inter alia, ensure that personal data is only processed if it is necessary having regard to the purpose of the processing.
SW-7	The controller shall, inter alia, ensure that personal data which is processed is correct and, if it is necessary, up-to-date.
SW-8	The controller shall, inter alia, ensure that personal data is rectified, blocked or erased, if it is incorrect or incomplete having regard to the purpose of the processing.
SW-9	The controller shall, inter alia, ensure that personal data is not kept for a longer period than is necessary.

Great Britain

GREAT BRITAIN (COP)	
COP -1	Information should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes.
COP-2	Access to information should be confined to those authorized to have it for the purpose for which it was supplied.
COP-3	The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose.
COP-4	In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.
COP-5	There should be arrangement whereby the subject could be told about the information held concerning him.
COP-6	The level of security to be achieved by a system should be specified in advance by the user and should include precautions against deliberate abuse or misuse of information.
COP-7	A monitoring system should be provided to facilitate the detection of any violation of the security system.
COP-8	In the design of information systems, periods should be specified beyond which the information should not be retained.
COP-9	Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.
COP-10	Care should be taken in coding value judgments.

EU Data Directive

EU DATA DIRECTIVE (95/46/EC)	
EU 95-1	Member States shall provide that personal data must be processed fairly and lawfully.
EU 95-2	Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.
EU 95-3	Member States shall provide that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
EU 95-4	Member States shall provide that personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
EU 95-5	Member States shall provide that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

EU DATA DIRECTIVE (2002/58/EC)	
EU 02-1	**Article 4 - Security** 1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. (Article 4, Security) 2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved. (Article 4, Security)
EU 02-2	**Article 5 -Confidentiality of the communications** 1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality. (Article 5, Confidentiality) 2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication. (Article 5, Confidentiality) 3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. (Article 5, Confidentiality)

EU 02-3	**Article 6 - Traffic data** 1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1). (Article 6, Traffic data) 2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued. (Article 6, Traffic data) 3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time. (Article 6, Traffic data) 4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3. (Article 6, Traffic data) 5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities. (Article 6, Traffic data) 6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes. (Article 6, Traffic data)
EU 02-4	**Article 8 - Presentation and restriction of calling and connected line identification** 1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the

	calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis. (Article 8, Caller ID) 2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls. (Article 8, Caller ID) 3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber. (Article 8, Caller ID) 4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user. (Article 8, Caller ID) 5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries. (Article 8, Caller ID) 6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4. (Article 8, Caller ID)
EU 02-5	**Article 9 - Location data other than traffic data** 1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. (Article 9, Location data) 2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or

	subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication. (Article 9, Location data) 3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service. (Article 9, Location data)
EU 02-6	**Article 12 - Directories of subscribers** 1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory. (Article 12, Directories) 2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge. (Article 12, Directories) 3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers. (Article 12, Directories) 4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected. (Article 12, Directories)
EU 02-7	**Article 13 - Unsolicited communications** 1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. (Article 13, Unsolicited communications). (Article 13, Unsolicited

	communications) 2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use. (Article 13, Unsolicited communications) 3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation. (Article 13, Unsolicited communications) 4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited. (Article 13, Unsolicited communications) 5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected. (Article 13, Unsolicited communications)

U.S. NSTIC

U. S. NSTIC (National Strategy for Trusted Identities in Cyberspace)	
N-1	**TRANSPARENCY**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information. (PII)
N-2	**INDIVIDUAL PARTICIPATION:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
N-3	**PURPOSE SPECIFICATION:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
N-4	**DATA MINIMIZATION:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
N-5	**USE LIMITATION:** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
N-6	**DATA QUALITY AND INTEGRITY:** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
N-7	**SECURITY:** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
N-8	**ACCOUNTABILITY AND AUDITING:** Organizations should be accountable for complying with these principles, providing training to all employee and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Council of Europe (COE)

COUNCIL OF EUROPE (COE)	
COE -1	Personal data undergoing automatic processing shall be obtained and processed fairly and lawfully.
COE-2	Personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.
COE-3	Personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored.
COE-4	Personal data undergoing automatic processing shall be accurate and, where necessary, kept up to date.
COE-5	Personal data undergoing automatic processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
COE-6	Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.
COE-7	Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.
COE-8	Any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file.
COE-9	Any person shall be enabled to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form.
COE-10	Any person shall be enabled to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention.
COE-11	Any person shall be enabled to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

OECD

OECD	
OECD-1	**COLLECTION LIMITATION PRINCIPLE:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
OECD-2	**DATA QUALITY PRINCIPLE:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
OECD-3	**PURPOSE SPECIFICATION PRINCIPLE:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
OECD-4	**USE LIMITATION PRINCIPLE:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.
OECD-5	**SECURITY SAFEGUARDS PRINCIPLE:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
OECD-6	**OPENNESS PRINCIPLE:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
OECD-7	**INDIVIDUAL PARTICIPATION PRINCIPLE:** An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
OECD-8	**ACCOUNTABILITY PRINCIPLE:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

HEW 1

HEW 1	
HEW 1	There must be no personal data record keeping systems whose very existence is secret.
HEW 2	There must be a way for an individual to find out what information about him is in a records and how it is used.
HEW 3	There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
HEW 4	There must be a way for an individual to correct or amend a record of identifiable information about him.
HEW 5	Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse.

PPSC

PPSC	
PPSC-1	**The Openness Principle** – There shall be no personal data record keeping system whose very existence is secret and there shall be a policy of openness about an organization's persona data record keeping policies, practices and systems.
PPSC-2	**The Individual Access Principle** – An individual about whom information is maintained by a record keeping organization in individually identifiable form shall have a right to see and copy that information.
PPSC-3	**The Individual Participation Principle –** An individual about whom information is maintained by a record keeping organization shall have a right to correct or amend the substance of that information.
PPSC-4	**The Collection Limitation Principle –** There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information.
PPSC-5	**The Use Limitation Principle –** There shall be limits on the internal uses of information about an individual within a record keeping organization.
PPSC-6	**The Disclosure Limitation Principle –** There shall be limits on the external disclosures of information about an individual a record keeping organization may make.
PPSC-7	**The Information Management Principle –** A record keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate.
PPSC-8	**The Accountability Principle –** A record keeping organization shall be accountable for its personal data record keeping policies, practices, and systems.

U.S. FTC

U.S. FTC	
FTC-1	**Notice:** data collectors must disclose their information practices before collecting personal information from consumers
FTC-2	**Choice:** consumers must be given option with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided
FTC-3	**Access:** consumers should be able to view and contest the accuracy and completeness of data collected about them
FTC-4	**Security:** data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use

OITF WP

OITF WP	
OITF-1	**Lawfulness:** OITF Providers are responsible for ensuring that the technical, operational, and legal requirements of the OITF are consistent with the laws of the jurisdiction(s) where parties use it to conduct exchanges involving identity information.
OITF-2	**Open reporting and publication**: OITF Providers must produce periodic reports on the operation and governance of the trust framework. They must ensure that a web site devoted to the OITF provides easy and timely access to (a) the periodic reports, (b) all agreements that constitute the legal structure of the trust framework, (c) all policies and procedures by which the OITF operates (including criteria and processes for certification), (d) a plain-language explanation of the trust framework's trust characteristics (for example, data protection strengths and weaknesses), and (e) records of dispute resolution activities and their results. However, publication is not required for assessment reports. OITF Providers must ensure that all parties to agreements under the OITF have visibility into who is participating in it and in what capacity.
OITF-3	**Ombudsmen:** OITF Providers must ask governments where they do business to designate independent ombudsmen whose role is to look after the interests of individual users under their respective jurisdictions, and they must ensure that the OITF is designed to allow these ombudsmen to do their job. If law requires the sharing of identity information (including biometric data, behavioral data, and social graphs) without the informed consent of the person in question, parties to the OITF who are ordered to share this information must involve the ombudsmen.
OITF-4	**Anti-circumvention and open disclosure:** OITF participant must not be party to any side agreements that compromise the integrity of commitments under the trust framework. If a participant is party to any agreements that might otherwise conflict with obligations under the trust framework, that party must disclose the existence and nature of these agreements to the affected party or parties at the earliest opportunity. OITF Providers and assessors must disclose all their agreements and the terms of those agreements.
OITF-5	**Non - discrimination.** Participants in the OITF must avoid discrimination. Participants must not engage in exclusive dealing arrangements relating to the trust framework.

OITF-6	**Interoperability.** Software and hardware specified in the technical requirements of an OITF must conform to defined standards that promote interoperability.
OITF-7	**Open Versioning:** OITF Providers must spell out how new versions of the OITF will be decided, when they will be published, how participants will be transitioned to these new versions, and how the interests of participants in the OITF will be protected.
OITF-8	**Participant Involvement:** OITF Providers must enable participants to share contact details so that they may convene virtually to discuss matters related to the trust framework.
OITF-9	**Data Protection.** Participants in OITFs will adhere to data protection practices at least as strong as those of the OECD's Privacy Guidelines (Part Two in its entirety, concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability).
OITF-10	**Accountability:** OITF Providers must state on a publicly accessible web site how the OITF provides accountability to all participants, including the users whose identity information will be exchanged under it.
OITF-11	**Auditability:** OITF Providers must ensure that all parties to agreements under the trust framework, including themselves, agree to be subject to audit for conformance with these Principles of Openness.
OITF-12	**Redress.** OITF Providers must ensure that all agreements under the OITF afford the parties an effective right and mechanism to seek redress.

U.S. DHS

U.S. DHS	
DHS-1	**Accountability and Auditing:** DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PH, and auditing the actual use of PH to demonstrate compliance with these principles and all applicable privacy protection requirements.
DHS-2	**Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
DHS-3	**Purpose Specification:** DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
DHS-4	**Data Minimization:** DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PH for as long as is necessary to fulfill the specified purpose(s).
DHS-5	**Security:** DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
DHS-6	**Use Limitation:** DHS should use PH solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
DHS-7	**Data Quality and Integrity:** DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
DHS-8	**Individual Participation:** DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

APEC

APEC (For the full text of each principle, see http://publications.apec.org/publication-detail.php?pub_id=390)	
A-1	**PREVENTING HARM**
A-2	**NOTICE**
A-3	**COLLECTION LIMITATION**
A-4	**USES OF PERSONAL INFORMATION**
A-5	**CHOICE**
A-6	**INTEGRITY OF PERSONAL INFORMATION**
A-7	**SECURITY SAFEGUARDS**
A-8	**ACCESS AND CORRECTION**
A-9	**ACCOUNTABILITY**

GSMA

GSMA (For the full text of each principle, see http://www.gsmworld.com/documents/GSMA_Privacy_Principles_UPDATED.pdf)	
GSMA-1	**OPENNESS, TRANSPARENCY AND NOTICE**
GSMA-2	**PURPOSE AND USE**
GSMA-3	**USER CHOICE AND CONTROL**
GSMA-4	**DATA MINIMIZATION AND RETENTION**
GSMA-5	**RESPECT USER RIGHTS**
GSMA-6	**SECURITY**
GSMA-7	**EDUCATION**
GSMA-8	**CHILDREN AND ADOLESCENTS**
GSMA-9	**ACCOUNTABILITY AND ENFORCEMENT**

Copyrights and Trademarks

Respect Network Corporation
12233 Corliss Avenue North, Seattle, WA 98133, USA