ISO/IEC JTC1 SC27 Privacy Standards

JPEG Privacy & Security 2nd Workshop 2016-02-23

Gregg Brown

Microsoft

Core components of ISO/IEC 29100

1. Context and Contents of ISO/IEC 29100
2. Evolution of Privacy Principles
3. New SC27 work item on de-identification

Core components of ISO/IEC 29100

1. Definitions for key entities in the privacy ecosystem
2. Considerations for recognizing PII
3. Requirements for safeguarding privacy
4. A discussion of the principles that should guide policy and practice

Key entities in the privacy ecosystem

1. The PII principal is the natural person to whom the personally identifiable information (PII) relates
2. The PII controller (or data controller in some jurisdictions) is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
3. The PII processor (or data processor in some jurisdictions) is any person (other than an employee of the PII controller) who processes data on behalf of the PII controller.
4. PII is any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

Key entities in the privacy ecosystem

1. The PII principal is the natural person to whom the personally identifiable information (PII) relates
2. The PII controller (or data controller in some jurisdictions) is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
3. The PII processor (or data processor in some jurisdictions) is any person (other than an employee of the PII controller) who processes data on behalf of the PII controller.
4. PII is any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

US Fair Information Practice Principles (FIPPs) 1974

1. **Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
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.
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.
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).
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.
6. **Data Quality and Integrity**: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
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.
8. **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

OECD privacy principles – I980

1. Collection Limitation: 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.
2. Data Quality: 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.
3. Purpose Specification: 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 fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation: 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.
5. Security Safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. Openness The re 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.
7. Individual Participation An individual should have the right: a) to…confirmation of whether or not the data controller has data relating to him, b) to have communicated to him data relating to him… d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. Accountability Principle A data controller should be accountable for complying with measures which give effect to the principles stated above.

UK Data Protection Act – 1995

The UK Data Protection Act implements the EU Data Protection Directive (95/46/EC):

1. Fairly and lawfully processed;
2. Obtained only for specified purposes and not further processed in a manner incompatible with those purposes;
3. Adequate, relevant and not excessive;
4. Accurate and up-to-date;
5. Not kept for longer than is necessary;
6. Processed in line with the rights afforded to individuals under the legislation, including the right of subject access;
7. Kept secure;
8. Not transferred to countries outside the European Economic Area (EEA)) without adequate protection.

ISO/IEC 29100 principles – 2011

Derived (mixed up) from OECD, EU, FIPPS, PIPEDA, Other sources

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

ISO/IEC 20889: Information technology — Security techniques — Privacy enhancing data de-identification techniques (WD)

ISO/IEC 20889 characterizes de-identification techniques for practitioners

- 'Pseudonymization' is just one technique (and has a different meaning than in GDPR).
- Additional categories: Masking, Generalization, Randomization, Aggregation.
- 'Anonymization' is not defined; data anonymity as a concept isn't addressed except for aggregated statistics.

Highlights the essential role of security and organizational measures to reduce the risk of re-identification

Focuses on tabular arrangement of identifiers and attributes

- A collection of JPEGS, as an example
- An image can be considered an identifier or a "quasi-identifier"—capable of identifying a data principle when combined with other data

SC 27 WG5, Working Draft: Great opportunity to participate, liaise