Framework to Advance Interoperable Rules (FAIR) on Privacy

1. Purpose

This framework is a robust, technology and business model-neutral approach for the protection of privacy and personal data that advances the interests of all stakeholders, including consumers, businesses, individuals, and governments.[1] The purpose of this framework is to inform the development of legislation or the promulgation of rules that enhance personal data protection, further the trust relationship between companies and their customers, and enable innovation while also avoiding regulatory fragmentation that undermines all three goals. Inspired by the Fair Information Practice Principles (FIPPs), Europe's General Data Protection Regulation (GDPR), and the Asia-Pacific Economic Cooperation's (APEC) Principles and Cross Border Privacy Rules (CBPR), this framework provides recommendations to both protect individuals' privacy and allow society to harness the potential of the digital age.[2]

While building on the strengths of existing global approaches, this framework is grounded in the principles of accountability, context, and mitigation of privacy risk to the individual and offers several key advantages including:

- creating alignment with the privacy protections of other privacy regimes across the globe and enabling interoperability with these global approaches;
- avoiding onerous process requirements that degrade the user experience, inject unnecessary costs into the ecosystem, or otherwise deter continued innovation and the participation of small- and medium-sized enterprises in the digital economy;
- encouraging innovation in and the adoption of security and privacy best practices by recognizing the benefits of techniques and controls that obstruct reidentification; and
- better enabling valuable research and innovation in areas such as machine learning and artificial intelligence that rely on the use of personal and non-personal data.

These elements advance both the rights of individuals and the responsibilities of entities in using personal data while sustaining the innovation necessary to deliver the products and services that consumers and businesses demand.

---

[1] Given existing laws governing the rights of individuals as employees, this framework does not apply in the employment context.

[2] In recognition of the need for government agencies and law enforcement or their third-party data processors to use personal data for the prevention, investigation, detection, or prosecution of criminal offenses; the execution of criminal penalties; or for preventing threats to public safety, data protection requirements and derogations for these purposes will need to be considered separately from this framework.

2. Defining Personal Data and Sensitive Personal Data

The foundational elements of any privacy policy framework are the definitions of "personal data" and "sensitive personal data." In this framework, "personal data" is any data that is reasonably linkable to or associated with, either directly or indirectly, a specific natural individual. "Sensitive personal data" is personal data consisting of ethnic origin, political affiliation, religious or philosophical belief, trade union membership, genetic data, biometric data, health data, sexual orientation, certain data of known minors, and precise geolocation data. Data that is anonymized, pseudonymized and protected, or otherwise publicly available is not personal data. Publicly available data means information that is lawfully made available in federal, state, or local government records, or that is lawfully made available to the general public.

3. Transparency

Individuals should be informed about the collection and use of their personal data in a fashion that is meaningful, clear, conspicuous, and useful to the individual. Such notices should be informed by state-of-the-art practices on effective disclosure, and include information regarding:

- the types of personal data collected;
- the entity that is collecting their personal data;
- how the personal data will be used;
- how long the personal data will be retained;
- whether and for what purposes personal data may be accessed by or transferred to third parties and the types or categories of third parties to whom such data may be transferred; and
- an explanation of control, choice, and redress mechanisms available to individuals.

4. Individual Control Rights and Context

Individuals should have the right to exercise control over the use of their personal data where reasonable to the context surrounding the use of personal data. These individual control rights, consistent with the rights and legal obligations of other stakeholders, include the right to access, correct, port, delete, consent, and object to the use of personal data about themselves.

Sensitive Data

Individuals should have the right to expressly and affirmatively consent to the use of their sensitive personal data, unless such use is necessary based on the context or otherwise permitted under applicable law.

Access, Objection, Correction, Deletion, and Portability Controls

Subject to the context considerations of the following subsection, where reasonable, individuals should have the right to the following:

- be informed about the categories of companies who are collecting their personal data and how they are using it;
- access in a timely manner personal data collected from them;
- object to the use of their personal data;
- rectify, complete, or delete inaccurate or incomplete personal data;
- have an entity delete their personal data; and
- obtain and port personal data that they provided to the entity across different services.

Enabling Context-Based Individual Control

While individual control mechanisms may differ in design features and deployment, and may also evolve over time, they should always provide individuals with reasonable transparency and the means to exercise the rights laid out above to the extent they are appropriate to the context surrounding the use of that personal data.

Key considerations in determining the appropriate level and means of enabling individuals to exercise control over the use of their personal data in a particular context should include, but are not limited to the:[3]

- extent, frequency, nature, and history of interactions between individuals and an entity, if any, and whether the personal data being used is inferred;
- expectations of reasonable users about how an entity uses their personal data, including through any notice it provided;
- extent to which personal data is exposed to public view;
- extent to which personal data is pseudonymized and the probability and ease of reversing that pseudonymization for any given entity that has access to such data;
- practical difficulty or infeasibility of accessing or deleting data from backup systems or archives, or segregating the individual's personal data from others in order to enable access;
- benefits to individuals and society of a certain use of personal data;
- types of personal data that need to be used for an entity's customary internal operations;
- age and sophistication of individuals to whom an entity targets or markets its goods or services, including whether it is directed toward minors or the elderly;
- sensitivity of the personal data being used;
- reasonably discernible potential privacy risks of an entity's planned use of personal

[3] We appreciate that some aspects of any privacy framework will necessitate regulatory rulemaking. Context is an area that is ripe for such rulemaking to ensure consideration of the factors identified in this framework as well as others that may be relevant (e.g., factors related to public safety).

data;[4] or

- extent to which personal data is processed to protect the vital interest of the individual or necessary for the performance of a task carried out in the interest of public safety, for law enforcement purposes, or in the exercise of the official authority vested in the controller entity.

5. Responsible Uses

For purposes of this framework, the term "use" is defined as all processing, collecting, handling, storing, retaining, disclosing, and transferring of personal data. This use concept is further refined by the entity's relationship to the data. For instance, liability and accountability obligations vary based on the extent to which the entity determines the purposes for and manner of use of the personal data. Where a company does not determine the purposes and manner of use of the personal data but has been contracted to use that data on behalf of another entity, that company acts as a service provider.

Using Data Responsibly

Companies should identify, monitor, and document uses of data they know to be personal and ensure that all identified uses of that personal data are legitimate. When acting as a service provider, companies should only use the personal data provided to them in accordance with the instructions of the entity that provided the data, and to assist that entity in meeting its privacy and security obligations.

Legitimate uses of personal data include those:

- that are appropriate to the context and where the associated privacy risk to individuals is negligible or has been minimized to a reasonable level;
- where the benefits to individuals and other stakeholders outweigh any potentially negative impacts on individuals and other stakeholders and where the associated privacy risk to individuals is negligible or has been minimized to a reasonable level;
- for which individuals have provided informed, freely given, and unambiguous consent;
- that are necessary to provide a requested good or service;
- that are for research and measurement purposes and where the data is protected through appropriate security measures;
- that ensure the efficient operation of devices, networks, and facilities, and where the associated privacy risk to individuals is negligible or has been minimized to a reasonable level; or

[4] Identification and classification of privacy risk factors would benefit from further collaborative development and guidance by all relevant stakeholders. In October 2018, NIST initiated a collaborative process to develop a privacy risk management framework to provide a catalog of privacy outcomes and approaches for all categories of entities to: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services.

- that are for specified public interest uses such as:
    - preventing or detecting fraud;
    - protecting the security of people, devices, networks, and facilities;
    - facilitating the efficient distribution of website and other internet content;
    - protecting the health, safety, rights, or property of the organization or another person;
    - mitigating institutional risk, including using, processing, or sharing of data for the purpose of protecting information systems and the data they store, process, and transport;
    - fulfilling contractual or other legal obligations; or
    - responding in good faith to valid legal process or providing information as otherwise required or authorized by law.

In addition to prohibitions of data use laid out in sectoral privacy laws, the use of data that is not captured by the above list of legitimate uses and where privacy risks cannot be mitigated to a reasonable level based on the context and where individuals have not provided informed consent should be prohibited. Regulatory authorities should be permitted to create specific public interest exemptions to this prohibition.

6. Risk Assessment and Mitigation

Companies should institute technical, contractual, and organizational measures and processes that comprehensively identify, assess, and monitor the privacy risk to individuals relating to the use of personal data, and should take reasonable steps to mitigate these risks. In doing so, companies should take into consideration the possible benefits of the personal data use to individuals, other stakeholders, and society at large. Privacy risk assessments may include reviews of data sources, systems, information flows, partnering entities, and data and analyses to examine the potential for privacy risk.

Companies should mitigate privacy risk to individuals by anonymizing, pseudonymizing where anonymization is not possible, or encrypting personal data whenever possible and appropriate to the context.

7. Security and Minimization

Companies should implement comprehensive security programs that are reasonable and proportionate to the size and complexity of their operations, the nature and scope of their activities, and the sensitivity of the personal information they knowingly use or that is under their control.

Security programs should be designed based upon an organization's risk profile and should include specific protections for an organization's most valuable data, which may include personal data, customer data, or business proprietary data. Security programs should be designed to prevent unauthorized access, use, or disclosure, as well as misuse, alteration, destruction, or other compromise of this data. Companies should regularly assess the sufficiency of any safeguards in place to prepare for

reasonably foreseeable internal and external risks.

Companies should ensure that personal data under their control is adequate (sufficient to properly fulfill the stated purpose), relevant (has a rational link to that purpose), limited to what is appropriate in relation to the purposes for which the data is used, and used only for purposes compatible with the context.

8. Disclosure of Personal Data to Service Providers

Companies providing access to or transferring personal data to a service provider should perform due diligence over such entities to ensure they have the appropriate procedures and controls in place to protect personal data. Companies should also require service providers to help them uphold these responsibilities via contractual commitments or other means, such as a recognized and enforceable self-certification program, and require service providers to notify them if they can no longer meet their obligations.

Liability among entities in the event of a breach of privacy or security should be allocated according to contractual agreements or, barring such agreements, according to the demonstrated fault giving rise to the breach event. When a service provider follows the instructions of the entity that provided the personal data, including the use of appropriate technical and organizational measures to ensure privacy and security, the service provider's responsibility under this framework is limited to meeting the obligations identified in the instructions provided by such entities.

In contrast, when personal data is transferred to another entity for that entity's own use, where it determines the purposes for and manner of use of such data, that entity is accountable for upholding the responsibilities articulated within this framework.

9. Accountability and Oversight

Companies should maintain records pertaining to risk assessments and security programs so that they are auditable by the designated authority in the event of an incident. The development of technical capacity within the oversight body to ensure robust enforcement of these principles is an important consideration in any privacy regime.

Individuals should have the right to redress mechanisms, such as complaint handling and resolution procedures, that ensure their rights are adequately protected and to be notified in a timely manner if a breach of their personal data triggers a risk of concrete and measurable harm to them or their rights.