Information Accountability Foundation

Adverse Processing Impact and Defining Risk

For a risk-based approach to data protection implementation and oversight to be effective, a definition for the negative consequences to be avoided is needed. It is necessary for such a definition to be broad enough to include the full range of potential negative outcomes to be managed and to be flexible enough for the prioritization necessary to be "effective by being selective."[1] The IAF model legislation, FAIR AND OPEN USE ACT, is risk-based with a broad requirement that covered entities conduct risk assessments to identify, avoid, manage and mitigate adverse processing impacts. It does not use the terms "harm" or "injury." Instead, the IAF model legislation defines a broad concept of "Adverse Processing Impact," which the IAF borrowed to create a basis for identifying and managing risk. The IAF's definition of Adverse Processing Impact aligns with the approach to privacy risk and "privacy problems" codified in the National Institute of Standards and Technology's publication, NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 2020. The definition of Adverse Processing Impact also is generally consistent with NIST's Catalog of Problematic Data Actions and Problems, which is a non-exhaustive, illustrative set of problematic data actions and problems that individuals could experience as the result of data processing.

The definition of "Adverse Processing Impact" in the IAF model legislation is as follows:

> ADVERSE PROCESSING IMPACT.— The term "Adverse Processing Impact" means detrimental, deleterious, or disadvantageous consequences to an Individual arising from the Processing of that Individual's Personal Data or to society from the Processing of Personal Data, including—
> 1. direct or indirect financial loss or economic harm;
> 2. physical harm, harassment, or threat to an Individual or property;
> 3. psychological harm, including anxiety, embarrassment, fear, and other mental trauma;
> 4. inconvenience or expenditure of time;
> 5. a negative outcome or decision with respect to an Individual's eligibility for a right, privilege, or benefit related to—
>   a. employment, including hiring, firing, promotion, demotion, reassignment, or compensation;

[1] Richard Thomas coined the term "effective to be selective" when he was the United Kingdom's Information Commissioner (ICO).

    b. credit and insurance, including denial of an application, obtaining less favorable terms, cancellation, or an unfavorable change in terms of coverage;
    c. housing;
    d. education admissions;
    e. financial aid;
    f. professional certification;
    g. issuance of a license; or
    h. the provision of health care and related services.
6. stigmatization or reputational injury;
7. disruption and intrusion from unwanted commercial communications or contacts;
8. discrimination in violation of Federal antidiscrimination laws or antidiscrimination laws of any State or political subdivision thereof;
9. loss of autonomy [2]through acts or practices that are not reasonably foreseeable by an Individual and that are intended to materially—
    i. alter that Individual's experiences;
    ii. limit that Individual's choices;
    iii. influence that Individual's responses; or
    iv. predetermine results or outcomes for that Individual; or[3]
10. other detrimental or negative consequences that affect an Individual's private life, privacy affairs, private family matters or similar concerns, including actions and communications within an Individual's home or similar physical, online, or digital location, where an Individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used.

Adverse processing impacts establish the basis for the organizational controls, assessment processes, engineering privacy by design, and review necessary for demonstrable accountability.

The relevant IAF documents, including the model legislation, a summary of the Risk of What paper, and this document may be found at informationaccountability.org/publications under the "Risk and Governance April 11, 2022" heading.

---

[2] The concept of "loss of autonomy" is widely recognized in many bills and frameworks including the NIST Privacy Framework, which provides that, "[l]oss of autonomy includes losing control over determinations about information processing or interactions with systems/products/services, as well as needless changes in ordinary behavior, including self-imposed restrictions on expression or civic engagement." Catalog of Problematic Data Actions and Problems.

[3] The IAF model legislation applies the well accepted drafting convention that "or" means "either or both", or if there is a series of items, "anyone item or combination of items".