

Framework for Responsible Data Protection Regulation

In our digital era, a growing array of organizations use personal data to provide a growing range of services. Responsible data use can unlock benefits for people, companies, and other organizations around the world. Regulation can protect individuals and communities from harm and misuse of data, and help maintain the trust that enables innovation and change. Building on our efforts to provide innovative services that rely on personal data, and on our experience with evolving international privacy laws, we have synthesized the following set of high-level principles. These principles are based on established privacy regimes and are meant to apply to organizations that make decisions regarding the collection and use of personal information. This framework helps Google evaluate legal proposals and advocate for smart, interoperable, and adaptable data protection regulations.

REQUIREMENTS

Collect and use personal information responsibly.

Organizations must operate with respect for individuals' interests when they process personal information. They must also take responsibility for using data in a way that provides value to individuals and society and minimizes the risk of harm based on the use of personal information (i.e., data that can be linked to a person or personal device).

Mandate transparency and help individuals be informed.

Organizations must be transparent about the types of personal information they collect, why they collect it, and how they use or disclose it, particularly when used to make decisions about the individual. Regulators should encourage organizations to actively inform individuals about data use in the context of the services themselves, helping to make the information relevant and actionable for individuals.

Place reasonable limitations on the manner and means of collecting, using, and disclosing personal information.

Collection and use of personal information can create beneficial and innovative services, within a framework of appropriate limits to the collection, use, and disclosure of personal information to ensure processing occurs in a manner compatible with individuals' interests and social benefits.

Maintain the quality of personal information.

Organizations should make reasonable efforts to keep personal information accurate, complete, and up-to-date to the extent relevant for the purposes for which it is maintained. Data access and correction tools, as mentioned below, can assist organizations in meeting this obligation.

Make it practical for individuals to control the use of personal information.

Organizations must provide appropriate mechanisms for individual control, including the opportunity to object to data processing where feasible in the context of the service. This does not require a specific consent or toggle for every use of data; in many cases, the processing of personal information is necessary to simply operate a service. Similarly, requiring individuals to

control every aspect of data processing can create a complex experience that diverts attention from the most important controls without corresponding benefits.

Give individuals the ability to access, correct, delete and download personal information about them.

Individuals must have access to personal information they have provided to an organization, and where practical, have that information corrected, deleted, and made available for export in a machine-readable format. This not only empowers individuals, it also keeps the market innovative, competitive, and open to new entrants.

Include requirements to secure personal information.

Organizations must implement reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, modification, and destruction, and should expeditiously notify individuals of security breaches that create significant risk of harm. Baseline precautions should apply to any collection of personal information, and additional measures should account for and be proportionate to the risk of harm.

SCOPE AND ACCOUNTABILITY

Hold organizations accountable for compliance.

Accountability can and should come in many forms. Lawmakers and regulators should set baseline requirements and enable flexibility in how to meet those requirements. Industry accountability programs and safe harbors can incentivize best practices, particularly in providing more flexible approaches to dealing with evolving technologies.

Focus on risk of harm to individuals and communities.

Regulators should encourage the design of products to avoid harm to individuals and communities. Enforcement and remedies should be proportional to the potential harms involved in the violation. Innovative uses of data shouldn't be presumptively unlawful just because they are unprecedented, but organizations must account for and mitigate potential harms. This includes taking particular care with sensitive information that can pose a significant risk. To enable organizations to develop effective mitigations, regulators should be clear about what constitutes a harm.

Distinguish direct consumer services from enterprise services.

Much processing of personal information is done by one company on behalf of another, where the processor lacks legal authority to make independent decisions about how to use the data or operate outside the bounds of the client's direction. Sometimes this distinction is described as "processors" versus "controllers", allowing for the efficient use of vetted, qualified vendors with minimal additional compliance costs, which is particularly important for smaller entities. Processors can look to the controller to meet certain obligations under the law, including transparency, control, and access, but processors must still meet basic programmatic and security responsibilities.

Define personal information flexibly to ensure the proper incentives and handling.

The scope of legislation should be broad enough to cover all information used to identify a specific user or personal device over time and data connected to those identifiers, while encouraging the use of less-identifying and less risky data where suitable. The law should clarify whether and how each provision should apply, including whether it applies to aggregated information, de-identified information, pseudonymous information or identified information.

Apply the rules to all organizations that process personal information.

Data is increasingly important through all sectors of the modern economy. Aside from the context of particular relationships that have existing rules, like with one's employer or attorney, legislation should apply to all economic sectors and all types of organizations that process personal information. While certain sectors (e.g., healthcare) may have additional rules, regulation should set a baseline for all organizations. The application of the law should also take into account the resource constraints of different organizations, encouraging new entrants and diverse and innovative approaches to compliance.

Design regulations to improve the ecosystem and accommodate changes in technology and norms.

The technology involved in data processing is not static, and neither are the social norms about what is private and how data should be protected. A baseline law can provide clarity, while ongoing reviews (e.g., rulemakings, codes of conduct, administrative hearings) can provide more flexible and detailed guidance that can be updated without wholesale restructuring of the legal framework. Governments can support these goals by rewarding research, best practices, and open-source frameworks. Creating incentives for organizations to advance the state of the art in privacy protection promotes responsible data collection and use.

Apply geographic scope that accords with international norms.

Data protection law should hew to established principles of territoriality, regulating businesses to the extent they are actively doing business within the jurisdiction. Extra-territorial application unnecessarily hampers the growth of new businesses and creates conflicts of law between jurisdictions. In particular, small businesses shouldn't have to worry about running afoul of foreign regulators merely because a few people from another country navigate to their website or use their service.

Encourage global interoperability.

Mechanisms allowing for cross-border data flows are critical to the modern economy. Organizations benefit from consistent compliance programs based on widely shared principles of data protection. Countries should adopt an integrated framework of privacy regulations, avoiding overlapping or inconsistent rules whenever possible. Regulators should avoid conflicting and unpredictable requirements, which lead to inefficiency and balkanization of services and create confusion in consumer expectations. In particular, geographic restrictions on data storage undermine security, service reliability, and business efficiency. Privacy regulation should support cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms that ensure protections follow the data, not national boundaries.