10 Goals for Good Privacy Protection Law

The concept of digital privacy refers to an individual's right to determine when, how, and to what extent their personal data can be collected and shared. Privacy is essential to our ability to trust the Internet. Without it, people, countries, and economies can't fully benefit from the opportunities the Internet can provide.

Large-scale corporate data breaches and inappropriate use of personal data seem to happen more often. It is more important than ever that laws created to protect us provide clear, achievable rules for privacy protection, and motivate data handlers to improve best practice. Legislation must also be technology neutral, so that it underpins lasting protection of personal data without harming the infrastructure of the Internet. Well-crafted legislative solutions will protect users, consider the evolving nature of technology, and encourage constructive and beneficial innovation.

A good privacy law should:

Require Privacy-by-Design

Require privacy-by-design, from the outset, when new products or services are developed. Privacy-by-design includes principles such as data minimization, clear specification of intended use, and limits on sharing and retention.

Promote Clarity

Require plain language on all privacy-related agreements, to ensure users can give informed consent based on a true understanding of what will be shared, how, and with whom.

Enforce Privacy Protection

Ensure that privacy regulation can be effectively enforced, and that data handlers are accountable for their privacy practices. Require safeguards to enhance data security overall, based on accepted best practice.

Strengthen Oversight and Enforcement

Undergo regular review to ensure that the law remains relevant and fit for purpose, provides sanctions and remedies for privacy violations, and encourages companies to be transparent about compliance.

Give Users Control

Give users effective control over their own privacy, requiring data handlers to give users greater control over whether, and how, personal data is shared, including the ability to opt out. If users opt to share data, the law should enable them to request its removal later. And if users opt out of sharing, this should not unnecessarily restrict their access to services.

Increase Accountability

Require transparency and accountability for privacy practices and breaches. If something goes wrong, data handlers must be held accountable and do their best to contain the harm, give appropriate support to help those affected, and ensure timely notification of any violations. The cost of bad practice must be borne by the responsible party.

Work Globally

Aim to achieve interoperability between different jurisdictions, so that personal data enjoys continuity of privacy protection as it crosses borders, without undermining the Internet's global nature.

Be Strict but Fair

Impose strict conditions on any exceptions to privacy and personal data protection. Exceptions should be restricted to matters of national security or public safety. They must have a legitimate goal, be necessary and proportionate, and be subject to transparent, independent judicial supervision.

Keep it Anonymous

Protect individuals and their data against the "re-identification" of private data over time. The law should require data handlers to ensure that privacy protection methods - including anonymization, where this is allowed as a privacy protection - remain reliable, as technology and re-identification methods evolve.

Be Drafted Collaboratively

Reflect the views of relevant stakeholders in the policy process. Privacy affects everyone, so it makes sense to engage the private sector, regulators, privacy advocates and consumer groups in formulating policy in this area. Multi-stakeholder participation makes for more open and sustainable policy-making.

internetsociety.org

Internet Society