10 Signs of a Good Privacy Protection Law/Policy

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

We are living in a time when large-scale corporate data breaches and inappropriate use of personal data seem to happen almost every day. It is more important than ever that laws and policies created to protect us provide clear, achievable rules for privacy protection that data handlers are proud to champion. They must also be technology neutral to promote relevant, lasting protection of user data in a way that does not harm the infrastructure of the Internet. Legislative solutions must fit technological realities to protect users and enhance—rather than impede—innovation.

A good privacy law or policy must:

Require Privacy-by-Design

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

Speak Clearly

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

Ensure privacy policies are enforced, and that they include accountability measures for personal data handling, and safeguards to enhance data security overall.

Strengthen oversight and enforcement

Review laws and policies regularly to ensure they are relevant and fit-for-purpose, provide sanctions and remedies for privacy violations, and encourage companies to be transparent about compliance.

Give Users Control

Give users greater control and choice over if and how they share their data. If users opt to share data, they should be able to request its removal later; and if they opt out, they should have meaningful alternatives. Easy-to-use privacy controls should also be provided.

Be Transparent

Require transparency and accountability for privacy practices and breaches for all public and private entities. 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.

Be Drafted Collaboratively

Privacy affects everyone, so it makes sense to involve the private sector, regulators, consumers groups and individuals in creating solutions. Multi-stakeholder participation makes for more open and sustainable policy-making.

Work Globally

The Internet is borderless, yet privacy and data protection laws are national. Special cross-border, mutually-agreed provisions are needed to protect personal data that leaves one country and enters another, to ensure continuity without undermining the Internet's global nature.

Be Strict but Fair

Limit exceptions to privacy and personal data protection laws to matters of national sovereignty, security or public safety. Any limits must have a legitimate goal, be necessary and proportionate. Allow transparent, independent judicial supervision of exceptions.

Keep it Anonymous

Protect individuals and their data against "re-identification" over time by ensuring anonymization methods are reliable. A person's privacy is at risk if personal data that has been scrubbed of identifying information can still be used by others to trace it back to them.