

Anatomy of a Privacy Law

by Daniel J. Solove

Scope and Applicability

- types of entities covered?
- size of entities covered?
- location of entities – extraterritorial applicability?

Definition of Personal Data

- recognizes identifiable data?
- recognizes category of sensitive data?

Basis of Processing

- requires legal basis to process data?
- types of legal bases?
- types of data processing without consent?
- data use restrictions even with consent?

Individual Rights

- transparency or notice provisions?
- right to access?
- right to correct?
- right to erasure or deletion?
- right to object to processing?
- right to data portability?

Consent

- definition of consent?
- opt-out consent? opt-in consent?
- restrictions on conditioning products or services on consent?

Children

- special provisions for parental consent for children?
- age of children?

Data De-Identification

- provisions for data de-identification, pseudonymization, or anonymization?

Security

- reasonableness? or specific security requirements?
- breach notification to authorities? notify individuals?



Responsibilities

- confidentiality?
- data minimization?
- data retention and destruction?
- database registration requirements?

Governance

- requires CPO or DPO?
- requires workforce training?
- requires written policies and procedures?
- requires risk assessments?
- privacy by design requirements?
- privacy by default requirements?

Vendor Management

- requires contracts with vendors (aka “processors” or “service providers”)?
- specific types of requirements in vendor contracts?
- direct enforcement against vendors?

Cross-Border Transfer

- restrictions on cross-border transfer?

Enforcement

- independent enforcement authority?
- implementing regulations?
- agency enforcement? state AG enforcement?
- enforcement against data processors?
- private right of action?
- fines?
- criminal penalties?
- safe harbors or cure periods?

Preemption

- preempts other laws?
- floor or ceiling?
- limited preemption?