

State of New York

Suggestions for Privacy Legislation

From Theodore Claypoole, Womble Bond Dickenson

1. Definitions

- a. **Affiliate** means a legal entity that controls, is controlled by, or is under common control with, another legal entity, where the entity holds itself out as affiliated or under common ownership such that a consumer acting reasonably under the circumstances would anticipate their personal data being provided to an affiliate.
- b. **Data Controller** is a Regulated Entity which, alone or jointly with others, determines the purposes and means of processing of personal data.
- c. **Data Processor** is a Regulated Entity which processes personal data on behalf of the Data Controller.
- d. **Data Subject** any person whose Protected Data is being collected, held or processed.
- e. **Protected Information** consists of the two categories of data:
 - i. **Personally Descriptive Information** is any information, including name, address, email address, IP address, device identification by which a Data Subject may be directly identified.
 - ii. **Transactional Data** is information describing any action taken by a Data Subject with a Data Controller, including purchases of goods or services, deliveries, questions, interactions with Data Controller staff or agents and browsing monitored or tracked by Data Controller.
- f. **Regulated Entities** are Data Controllers and Data Processors which are for-profit companies with at least \$20,000,000 in gross revenue per year.
- g. **Transfer** means to change Protected Information's place, route, or means to a different entity.

2. Responsible Data Holder.

- a. Each Regulated Entity will be held to the standard of Responsible Data Holder under New York law.
- b. A Responsible Data Holder will not Transfer the Protected Information in its possession to any Person or Entity
- c. A Responsible Data Holder is must create a program to protect the security and confidentiality of the information, protect against any anticipated threats or hazards to the security or integrity of the information, as well as protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

- d. Responsible Data Holders may share Protected Information with other Data Controllers and Data Processors under agreements that protect the Protected Information and offer the same rights to Data Subjects as Provided in this Act.
- e. If a Responsible Data Holder is treating and guarding Protected Data within the constraints of this Act, then the Responsible Data Holder may otherwise use the Protected Data for its own business purposes, including marketing to the described Data Subject.
- f. A Responsible Data Holder securing Protected Data in a manner that contains administrative, technical and physical safeguards for the protection of personal information, and reasonably conforms to one of the “industry-recognized” cybersecurity frameworks enumerated in the law shall constitute an affirmative defense to a suit based on the lack of reasonable protection for Protected Data from third party access.

3. Data Subject Data Rights.

- a. Data Subjects have the following rights in regard to their own Protected Data with respect to Data Controllers and Data Processors:
 - i. Right to know what information is collected or held and tied to my identifier
 - ii. Right to correct wrong information
 - iii. Right to be excluded from marketing
 - iv. Right to be excluded from transfer of Personal Data to other Data Controllers
 - v. Right to eliminate data not used for non-marketing business purposes