Financial Data and Technology Association

http://www.fdata.global/north-america

# FDATA North America Privacy Principles

March 2023

FDATA North America's Privacy Working Group has cooperatively developed these principles to govern the usage, disclosures, liability, oversight, and technology involved in open finance ecosystems.

The first section of this document includes definitions of data types, and requirements for minimization, secondary usage, and silent parties. The second section covers consumers disclosures, what elements they should include, their length, and options for consumer revocation. The third section discusses assessments of data breach liability, notification requirements, and consumer redress. The fourth section covers regulatory oversight and suggests which regulators in the U.S. and Canada should be granted supervisory authority over data privacy to ensure that consumers, data providers, and third-parties are protected and acting responsibly. The final section covers the technology involved in user authentication and authorization, and how they can be changed and revoked by consumers.

Financial Data and Technology Association

http://www.fdata.global/north-america

# Contents:

Financial Data and Technology Association

http://www.fdata.global/north-america

# 1. Data Usage

### (a) Definitions

- **User-directed data** is data that is collected or shared in accordance with a clear affirmative action by or request from an end user or their authorized agent, rather than data collected passively, such as data that may be collected automatically through pixels or cookies as a consumer navigates through web pages.
    - The end user must have full utility over any non-proprietary data element for which a dataholder holds about them, for avoidance of doubt, including PII such as account number, which must include the ability to share those data elements digitally with third parties of their choosing.
    - The end user must have the ability to opt-out of future use of their data at any time.
- **Proprietary data** is data that a data holder can not be reasonably expected to allow their customers to share. This may include, for example, a stock ticker price that a data holder licenses from a third party. Proprietary data does not include data elements that are required to be disclosed to the customer. This includes, for example, fees and interest rates.
- **Derived data** is distinct from user-directed data. Derived data is data created when a data holder applies analytics to customer data, creating a new data element. Once a bank runs a KYC check on that data, for example, a second data type is produced that is derived.

- **Anonymized data** is a single data element or a data set that cannot reasonably be reidentified back to an individual end user.[1] A lawful basis and transparency to the user must be provided in order to process customer data into anonymized data.

**(b) Data minimization**:
If data is reasonably necessary to provide and/or improve service/product customer has opted into, and the customer has been made aware that the data is being collected, the dataholder should not restrict the ability of their customer to permission access to the data.

**(c) Secondary Usage:**
Anonymized data may be used for secondary use cases. The end user must be informed that data may be anonymized and be used for other purposes as allowed by law. Usage of anonymized data for secondary use cases should not be permitted for use cases intended to target or identify individual users.

User-permissioned data may be utilized for secondary use cases in limited circumstances, including compliance with legal orders, regulatory expectations, to protect the user and/or the integrity of the dataholder's or its partners 'systems, or, with reasonable notice, to develop new products or services.

**(d) Silent Parties**
A silent party is an individual whose data is included in the customer-permissioned data of another individual, but is not an accountholder on an account for which a customer provided their consent for their data to be collected. Silent party data may not be used for marketing, advertising or lead generation purposes.

[1] This definition is consistent with the Federal Trade Commission's guidelines regarding anonymized data as articulated in a 2012 report.

To the extent data collection or connectivity of a consenting user includes information about a silent party, such collection or connectivity should be permitted but data access should be limited to usage only for the product, service, or tool to which the consenting user opted into, except for compliance with legal orders, regulatory expectations, or to protect against or prevent fraud.

## 2. Disclosures

Disclosure should be made in a clear and concise manner by the entity directly providing a product or service to the consumer/SME as reasonably close in time and before the consumer's data is accessed to:

- The name of the product or service the end user is opting into, a description of that product or service and its legitimate business purpose.
- The name and contact details of the entity providing the product or service.
- Categories of data being permissioned, utilizing industry or regulatory standardized categories where possible. Particularly sensitive data fields, such as social security number, account number, or passport number, should be specifically called out.
- The length of time for which the end user is providing access to their data, the length of time that data will be retained, and the duration of the product or service for which the end user is opting into.
- How the end user may opt out of permissioning access to their data and the impact that may have on their use of the product or service, if applicable.
- [If applicable] That user-permissioned data will be used for product development.
- [If applicable] That user-permissioned data will be anonymized and used for other purposes as allowed by law.

- [If applicable] That the data recipient may provide access to user-permissioned data to additional parties, and the names of the additional parties who are acting as controllers with which the data will be shared, and for what purpose the data will be shared with the controller(s).

## 3. Liability

- The entity responsible for a data breach that results in financial loss for a consumer/SME is the entity that is liable to make that consumer/SME whole.
- It is the responsibility of an entity that has suffered a data breach to notify impacted consumers/SMEs, either directly or through a service provider. Such notification must include a summary of what data was accessed/lost and potential steps impacted consumers/SMEs may take to mitigate financial harm as a result of the breach.
    - Parties in the ecosystem should make reasonable efforts to cooperate with an entity that has suffered a data breach to assist in identifying impacted consumers/SMEs.
- Consumers/SMEs should be afforded the presumption of being eligible for reconstitution when they request remuneration for financial loss as a result of a data breach, subject to the following requirements:
    - The impacted consumer/SME must be provided a minimum of one year from the date a financial loss was experienced as a result of fraud or a data breach to request recompensation.
    - The impacted consumer/SME must demonstrate a connection between their financial loss and a data breach (e.g. that they held an account at an entity that experienced a breach).
    - Consumers/SMEs should not be eligible for recompensation of financial losses for authorized or first-party fraud provided the entity or entities through which the fraud was facilitated deployed reasonable anti-fraud and/or security protections.

- Entities that have suffered a data breach that has not resulted in any consumers/SMEs directly suffering financial loss should offer credit monitoring services to consumers/SMEs whose data was affected by the breach.
- A third party that has experienced a data breach as a result of a malicious attack must notify their data aggregator(s) after identification of the breach as soon as practicable or, in any event, within 24 hours. In such instances, data providers to that third party should be notified of the breach, either by the aggregator or, at the aggregator's direction, via the third party, subject to applicable regulatory or legal requirements.

## 4. Oversight

- To provide for uniform customer protection, policymakers in both Canada and the United States should enact broadly preemptive, federal data privacy regimes that provide consistent data privacy and customer data control.
- In both Canada and the United States, any such federal data privacy frameworks should grant existing federal regulatory agencies with the exclusive authority to implement, oversee, and enforce the data privacy statute.
    - In Canada, the Office of the Privacy Commissioner should be responsible for overseeing and enforcing a federal financial data privacy statute.
    - In the United States, the Consumer Financial Protection Bureau should be responsible for overseeing and enforcing a federal financial data privacy statute.
- In implementing a federal data privacy standard, regulators should exert direct supervision of data aggregation platforms and third parties should be subject to consistent data privacy standards that account for the varying types, sizes, and risk profiles of third-party use cases.

  - In the United States, the CFPB should use its existing regulatory authority to supervise data aggregators.
  - In Canada, the Open Banking accreditation requirements should subject data aggregators to a different set of requirements from non-aggregator third parties.
- In the event of a material security or privacy incident presented by an accredited third party, the governance entity of an open banking system may direct data access by that third party to be restricted until such time as the material security or privacy risk is addressed.
- A robust federal data privacy regime that empowers federal agencies to enforce a customer-protective data privacy environment need not include a private right of action.

# 5. Technology

**(a) Authentication:**

- Authentication is the process of validating the end user who wishes to access an account and validating any entity that is authorized to access data on behalf of the consumer.
- To the extent credential-based authentication is utilized for authenticating an end user, the data aggregator and/or third party should only retain an end user's credentials for as long as necessary to deliver the product, tool, or service for which the end user has opted into.
- Any authentication regime in an open banking environment must be secure and provide substantially the same authentication experience as the data provider's customer-facing online banking portal.
- Data providers should be prohibited from marketing to end users in an end user authentication flow.

**(b) Authorization:**

- Authorization is the process of the authenticated end user controlling which third parties may access certain elements of their data.
- A data provider may not override an end user's authorization to share data with an accredited third party.
- Authorization should occur at the third party that is carrying out a consumer's access request. This can be the data recipient, or data intermediary acting on the data recipient's behalf.
- Data authorized by an end user to a third party may only be used for the particular use case(s) authorized by that end user.
- Data recipients may not share an end user's data, or access to their data, with additional parties without the authorization of the end user.
- Once provided, customer authorization should persist until the customer revokes that authorization unless a material security issue requires a mandated re-authorization.
- Customers should have the ability to manage all of their authorizations in real-time.