FINANCIAL™ DATA EXCHANGE

Data Minimization Guidelines

Version 1.0
June 2023

Legal Notice

Financial Data Exchange, LLC (FDX) is a standards body and adopts this Data Minimization Guidelines for general use among industry stakeholders. Many of the terms, however, are subject to additional interpretations under prevailing laws, industry norms, and/or governmental regulations. While referencing certain laws that may be applicable, readers, users, members, or any other parties should seek legal advice of counsel relating to their particular practices and applicable laws in the jurisdictions where they do business. See FDX's complete Legal Disclaimer located at http://www.financialdataexchange.org for other applicable disclaimers.

Revision History

Document Version	Notes	Date
1.0	Initial Document Release	**June 2023**

Contents

Introduction to Data Minimization

Data minimization is an important concept to uphold throughout any financial data sharing interaction among participants as it reduces risk, limits exposure, and engenders trust. Everyone is safer if the amount of data being shared across the system is reduced to only the data needed to deliver the service, and with the End User's permission.

The FDX principle of Data Minimization asserts **that data shared between parties should be limited to that which is directly relevant and necessary to accomplish the specific purpose as consented by an End User**. Entities within the FDX ecosystem should endeavor to eliminate any extraneous data provided or received that is not required or was not authorized by the End User to be shared. Once data has fulfilled its intended purpose, it should be deleted, unless required for legal or regulatory record-keeping purposes. This is largely in-line with definitions published elsewhere and utilized in regulatory schemes such as that in the UK and EU.

The critical concept codified within this Data Minimization principle is that End Users have the right to grant access to their data. Information is shared only at the explicit direction of the End User and for a specific use or set of uses. All participants must adhere to contents and terms disclosed to the End User in the Consent.

The FDX Data Minimization principle should always apply across the ecosystem. It should be reflected in all standards and become an integral part of certification. While the history of data minimization is rooted in privacy frameworks such as the UK PSD2 and GDPR, FDX should uphold this principle independently of consumer data access rulemaking in the US and Canada. The FDX Data Minimization principle is not expected to run counter to any new regulations and may even exceed legislated standards.

Data Minimization Throughout the Data Sharing Lifecycle

There are opportunities to apply the FDX Data Minimization principle tactically throughout a typical data sharing life cycle. The FDX Data Minimization Guidelines highlight key data minimization methods, but encourage all FDX Working Groups to consider how they might operationalize them in practice and codify it to a greater level of detail. Any time there is a movement of data from one party to another, there is an opportunity to consider the minimum data needed and shed any excess information which may have been shared. And in the final stage, once the data has served its intended purpose, we see another opportunity to purge unnecessary data and remove it from the ecosystem , unless required for legal or regulatory record-keeping purposes.

Data Minimization Through Client Registration at the Data Provider

The Data Recipient may register with the Data Provider or Data Access Platform on its behalf for the data they may access for a use case. For example, the Data Recipient may register for access to the data to fulfill certain use cases, such as PFM or account aggregation applications, which would access a subset of all data available at the Data Provider for an end user. When the Data Provider issues the Token to access the End User's data, the data permissioned to the Token should not exceed the scope of the Data Recipient registered data scopes.

End User Provides Consent to Share Data

The data sharing life cycle begins with the capture of an explicit End User Consent granted for data to be shared, documented through the consent Data Cluster(s) and should be within the context of a use case or purpose described by the Data Recipient and/or Data Access Platform.

Context for the data share can be established through the Data Recipient Registration process, or through use case and scope parameters supplied to the Data Provider. The Data Recipient or Data Access Platform should communicate to the Data Provider the smallest possible scope of data requested so that the End User does not over-consent. Data scopes sent in the Consent API (OAuth2/PAR) must not exceed the scope of data or Data Clusters presented in the Consent user experience. The accurate description of what data will be shared is of paramount importance.

The Data Provider uses information from the Consent grant to determine what data is shared with the Data Access Platform or Data Recipient. Information in the explicit Consent grant should include:

- Data set(s) and/ or data elements to be shared
- Accounts to be shared[1]
- From whom, with whom, through whom
- For what duration
- For what lookback period, if applicable

Before allowing access to any End User data then, the Data Provider must ensure that there is an Active Consent record present.

FDX Data Minimization Methods

The FDX Data Minimization Guidelines identify methods leveraging FDX standards approved or in development for minimizing data. In all cases, data minimization begins with the End User having visibility to the data at the Data Provider for which they will grant access to the Data

[1] The Data Access Platform or Data Recipient only know about accounts authorized under the Consent at the end of the initial data access journey, when they obtain the list of accounts authorized under the Consent from the Data Provider.

Access Platform or Data Recipient. FDX uses the Data Cluster to inform the End User of the data requested to be accessed.

The following methods should be used in combination with Data Clusters or with each other to further minimize data:

1. **Data Cluster and Token claims and scope parity**: the OAuth2 or OpenID Connect (FAPIv1) scopes or claims must align with the scope of data represented in the Data Clusters presented to the End User in the Consent.
2. **Data Cluster and use of data**: how the data will be used by the Data Recipient (or Data Access Platform) application shall be consistent with the scope of data identified through the Data Cluster(s).
3. **Data Deletion at the Data Access Platform or Data Recipient**: the Data Access Platform only uses the data they access as required by the Data Access Platform service which is used by the Data Recipient; the Data Recipient only uses the data required by the Data Recipient Application. Once the data is no longer needed, it should be deleted.

Data Provider Shares the Permissioned Data

This is the most crucial phase for data minimization, as reduction of any unnecessary data sharing the furthest upstream will minimize risk in all subsequent interactions throughout the ecosystem, and is the first opportunity to honor restrictions per the Consent granted by the End User. The Data Provider should look at the data set defined by the Data Cluster(s) requested by Data Recipient or Data Access Platform either through OAuth2 or Consent API claims and scope against pre-defined data sharing registration with the Data Provider.

Once the data has been screened through data scopes, Data Clusters and use cases, any additional limitations set by the End User through the authorization process should then be applied to ensure only the consented account data is exposed, for the appropriate look back period, and for the consented duration.

Data Access Platform Accesses and Shares the Permissioned Data

Data Access Platforms facilitate financial data sharing for one or more Data Recipients and their underlying End Users. Data Access Platforms are responsible for minimizing the data they access to the scope of data available through the data services which are used by and documented to their Data Recipient clients.

Data Clusters or data scopes requested by the Data Access Platform (whether using a single- or multi-token integration) may necessarily be broader than the data set required to satisfy the needs of a single downstream Data Recipient, since there may be multiple Data Recipients and therefore use cases for the same End User that the data must cover. Before making data available to the Data Recipient, the Data Access Platform must minimize it further to align with the specific scope and use case needed.

Sensitive data should be treated with utmost caution due to the inherent risk posed by the proliferation of such data. Any excess Personal Identifiable Information (PII) that is shared by the Data Provider due to issues such as misalignment of data clusters to Data Provider endpoints should be immediately deleted by the Data Access Platform.

Often, the use case for a particular data set may dictate that only data from certain account types are needed, for example, checking accounts for a money movement use case, credit cards for a rewards comparison tool, or investment accounts for an equity trading compliance application. In this case, data should only be returned by the Data Provider or retained by Data Access Platform or Data Recipient for the accounts compatible with the data.

Data Access Platforms play a role in controlling the cadence with which data is obtained on behalf of their Data Recipients clients. This cadence should align to the consent granted by the End User. A data share with one time access granted should not be persisted, nor a time bound share accessed beyond the consented end date. Where there are multiple data shares by the same End User, time duration enforcement and data minimization policies normally used by the Data Provider may not be viable in some circumstances, so it is incumbent on the Data Access Platform in these circumstances to adhere to the data minimization principles. This same guidance applies to lookback periods.

Data Access Platforms offer a variety of commercial products that may tie to different data sets. These DAP data sets may differ from the FDX Data Clusters or other structures used by the Data Providers to organize the data shared. In this scenario, multiple Data Clusters may need to be used in order to pull out and recombine the relevant data elements needed for the DAP data set. Here, the Data Access Platform has the responsibility to delete any extraneous data that is not required in order to deliver the product and minimize the data shared to just what is required.

Data Providers may have different mechanisms or tools which allow any data recipient to further refine the data accessed for an End User. Wherever and whenever possible, Data Access Platforms should avail themselves of these tools in order to minimize the data leaving the Provider. The earlier in the data sharing lifecycle that unneeded data is left behind or deleted, the better.

Data Recipient Application Uses the Permissioned Data

Data Recipients may either directly integrate with a Data Provider or utilize a Data Access Platform. The Data Recipient is the last stop for the consented data and this is where it will be used in service to the End User.

For direct Data Recipient integrations, the data minimization standards and responsibilities are identical to those described for Data Access Platforms; the Data Recipient uses only the data required by the Data Recipient Application and deletes any data not needed.

Data Recipients using a Data Access Platform must develop a similar set of data minimization controls at the most fine- grained level, since they alone know the precise data that is directly relevant and necessary to accomplish the specific purpose as consented by an End User.

Data Deletion to End the Lifecycle

Per the Data Minimization principles, once data has accomplished the specific purpose for which it was intended or if is otherwise no longer needed, it should be expunged, unless required for legal or regulatory record-keeping purposes. This should be done as a matter of course across Data Access Providers and Data Recipients.

All entities in the data sharing ecosystem should have clear policies directing the deletion of data. Data Recipients and Data Access Platforms should provide a mechanism for End Users to proactively request deletion of data that has been shared through their open banking connection, subject to what is required to be retained by legal or regulatory compliance.

Data Recipients working with Data Access Platforms should have a system in place which allows the Data Recipient to notify the Data Access Platform that an End User has instructed the Data Recipient to delete their data. The Data Access Platform must subsequently delete the same user data within the Data Access Platform, linked to the Data Recipient deleted data.

Data deletion ends the data sharing lifecycle and with it, ends concern around data minimization.

Conclusion

Data minimization is an important and expansive topic as it can be affected in many ways and across many touchpoints in open banking. This document marks the initial definition of a Data Minimization Principle for FDX as an organization. Herein we have laid out initial guidance and suggestions for where and how this principle can be put into practice. There are several areas where Working Groups can drive changes to FDX features and practices to incorporate data minimization.

Further discussions around data minimization are expected as are future versions and further refinements to the FDX Data Minimization Principle as the thinking and capabilities around it evolve over time. We look forward to strengthening the practice of data minimization alongside them.