

Design Note

DFSP GDD Collection

Guidance for DFSPs on how to collect and use gender data while safeguarding end-user privacy.

Gender Data Collection Should Happen Upfront

DFSPs should identify users' gender during the account sign up process. Where KYC is based on a digital national ID, providers have an opportunity to consistently pull gender information from the national ID database. In other cases, providers may need to ask users to provide their gender. Regardless, collecting this information upfront is imperative. Providers should also think through how to consistently apply a gender identifier to business accounts and joint accounts, both of which may introduce added complexity.

However, existing accounts may not have been set up with a gender identifier. In these cases, AI tools may enable providers to identify the gender of a previously unidentified accountholder.

Data Collected Should Be Usable and Applicable

Collecting GDD is not useful if the data is not used on an ongoing basis for the benefit of understanding end users. To facilitate this, the data needs to be stored in such a way that it can be easily accessed (in line with data protection rules) and analyzed along with other metrics. For example, account holders' gender data should be able to be matched with and relatable to broader account ownership and usage metrics, as well as other metrics such as alias usage and complaint and resolution data. The approaches to data usage should support reporting to the Inclusive IPS and regulators as well as usage by DFSPs to develop gender-responsive products and services.

Data Protection Is Valued by Women and Imperative for Women's Safety

Women are often more aware of risks related to data collection and usage. Providers should adhere to local privacy regulations and clearly and thoughtfully communicate why gender information is being collected and how it will be used. Providers should also help users understand how their data will be treated after they are no longer customers.