



---

STANDARDS FOR RESPONSIBLE DIGITAL FINANCIAL SERVICES:  
DATA RIGHTS & PRIVACY STANDARDS SECTION

---

8 June 2022

DRAFT

## CERISE + SPTF

### Draft Standards: Data Rights & Privacy

(as of 8 June 2022)

*Note: The Universal Standards for Social and Environmental Performance Management already contain a standard, with associated practices, on data rights and privacy. During the DFS standards working group discussion, the group validated that those practices are still relevant. The table below reminds us of what they are. The section “Standards for Data Rights & Privacy” below the table presents the additional standards that the group suggests could be relevant specific to a provider that delivers its products and services digitally.*

4.D.2	EP	The provider informs clients about data privacy and data rights.
4.D.2.1	Indicator	The provider explains to clients how it will use client data, with whom it will share the data, and how third parties will use the data. The provider receives clients' consent before using or sharing their data.
4.D.2.2	Indicator	Information about data use and consent is easy for clients to understand.
4.D.2.2.1	Detail	When requesting consent from clients to use their data, the provider explains in simple, local language, either in writing or orally, how it will use the data. Internet links to disclosure statements are not sufficient.
4.D.2.2.2	Detail	The provider trains clients on the importance of protecting their personal information including Personal Identification Numbers (PINs), savings account balances and information on repayment problems.
4.D.2.2.3	Detail	The provider gives clients the right to withdraw their permission to use data and explains any consequences of withdrawal.
4.D.2.3	Indicator	The provider notifies clients of their right to review and correct their personal and financial data.

#### **Standards for Data Rights & Privacy**

1. Inform customers of the benefits to them of agreeing to share their data, and explain to customers the consequences of opting out of data sharing.
2. Make it an opt-in option for customers to share their data.
3. Collect the minimum amount of data you need from customers.\*
  - \* define the “minimum” data as the data you use to make a decision about whether to offer them a product or service, and at what price
4. Have a system for how to receive and process customer requests to correct inaccurate information you (the FSP) have about them, and inform customers of this system.
5. If you deny an application for a product, explain to the customer why you denied it.
6. The leadership of the FSP defines a strategy for how the FSP processes and uses data, and monitors the implementation of those practices.

#### **Guidance on data rights & privacy: concepts, examples of real practice, and questions to address**

##### Concepts

- Data rights and privacy questions are strongly linked to governance. It is not enough to have the policies in place. The governing body(ies) of the FSP should take an active role regarding respecting customers’ data privacy and rights.

- All of the information shared with clients about how the FSP uses and shares data should be as simple as possible. If it is complicated to explain, it is not acceptable.

#### Examples of real practice:

- Interesting ideas on what type of information to provide that would be sufficient, from research in Rwanda presented at CFI 2021: “Sixteen participants out of the 30 had the experience of being rejected for a digital loan, and 10 of those recalled receiving an explanation for the denial. A few rejected applicants described a somewhat basic explanation such as, “Your credit limit is zero,” without further details, while others recounted more detailed instructions to “clear the balance on a previous unpaid loan,” before reapplying. “I only saw a message saying that I need to use Mokash for at least three months before applying for a loan,” said a 29-year-old female respondent. Six of the 10 participants who received an explanation were not satisfied with the provider’s communication. Despite mixed reviews of the provider’s explanation, eight out of the 10 respondents who recalled receiving explanations changed their behavior in response. Some began repaying their existing digital loans in a timelier fashion, while others increased savings and transactions within their mobile wallets.”
- Possible case study: Tala informs customers of what data it collects on them and how it uses it. For example, it offers explanations with icons to help customers understand why it is asking for their contacts list.

#### Outstanding questions:

- It is acceptable to follow an opt-out policy, meaning the customer is assumed to agree to data sharing unless s/he notifies the FSP that s/he is opting out? Or should the universal standard be an opt-in policy, meaning the FSP does not have the right to customer data, such as scraping data from customers’ phones, unless the customer opts-in to sharing those data?
- Interviewees had split opinions about consent. Some said customers should tick a box to give permission for every type of data the FSP wants to gain access to, while others said nobody is ever going to read that and it’s up to the provider to be responsible.