The LDP Process

The goal of Lean Data Practices (LDP) is to help you increase user trust and lower your operational risk by making smart, consistent decisions about data.

**Step 1: Assign someone to run point.** There should be a single person responsible for decisions about data who will manage steps 2 and 3 below (we’ll call her your “Data Steward”).

* 1. In a small startup: Ideally, you would tap an engineer or someone who already knows a lot about what data your organization collects and why. This is unlikely to be her only role, but it should be an important part of her job.
  2. Somewhere bigger: In this case you should consider establishing a role that is empowered to analyze and convene decisions about data across your organization (including engineering, marketing and other teams).

**Step 2: Make sure your Data Steward knows your data.** Understanding what user data you have and what you do with it is the next step to getting lean. Ask your Data Steward to think about the data they know and to interview people who make decisions about data using the [Lean Data Worksheet](https://github.com/mozilla/lean-data-practices/raw/master/Lean Data Worksheet.xlsx) as a guide. Remember to think about more than just your products and engineering — other functions (such as marketing, sales, etc.) sometimes collect and use user data.

**Step 3: Apply LDP.** Based on the results of Step 2, get lean by making changes to your data practices.

1. **Stay lean** by only collecting or keeping data you need. For each row on the worksheet, ask yourself:
   1. **Do I need this data to market or provide my business or product?** If not, you should try to stop collecting it or get rid of it. You may have to write a script that actively purges that data or modify your product so it doesn’t send that data to you in the first place.
   2. **How long do I need to keep it?** Sometimes you need raw data for a long time, but in many cases, it becomes of little value after a certain point. Plan a point in time where you do one of the following: (i) aggregate the data so it is no longer tied to specific users; and/or (ii) purge some or all of the data from your databases.
2. **Build in security**: Protect the data you store. For each piece of data, ask yourself:
   1. **Who needs access?** Try to limit access to those who truly need it.
   2. **Is the data stored securely? Should it be encrypted?** Depending on how you use the data and what it’s about, different levels of encryption may or may not be appropriate. The more sensitive the data, the more you should think about encrypting it while it’s being transferred and at rest.
3. **Engage your users:** Explain your practices simply. Ask yourself:
   1. **Is the way I collect, use and disclose data clear to my users?** If not, find a better way to communicate (through privacy policies, in product notices, etc.) so user expectation matches reality.
   2. **Do my users have options or control around their data?** Try to give your users ways to turn the data collection on or off and to express their preferences regarding how data is handled so you can respond accordingly.

**Go further.** Once you know your data and have applied LDP, you can generalize them and start to standardize a set of practices that your organization can follow moving forward.