The following analysis of DP-3T was made through the scope of the 6 strategies that ultimately form the data privacy by design & by default goal.

1. Strategy 1: Minimizing Collection
   1. The only data that DP-3T operates on is unique, random strings that are broadcasted to other phones in the vicinity that have the application installed. It does not collect location, user data or anything that would affect user privacy. Its sole purpose is contact tracing. Your application generates and broadcasts these strings, called “EphIDs” and simultaneously listens and collects to EphIDs generated by applications in range.
2. Strategy 2: Minimizing Disclosure
   1. The only disclosed data is the random unique strings, and when proven to the app that you’re covid +, your EphID is uploaded so that the people you’ve been in contact with get notified and no one else. Every user that has your EphID will get notified. Only the EphIDs of the infected user get uploaded to the central server.
3. Strategy 3: Minimizing Linkability
   1. Nothing can be linked or derived from the EphIDs that are on the central server, and the contact validation is done by the applications and not the server, therefore making it impossible to get anything from the EphIDs publicly available.
4. Strategy 4: Minimizing Centralization
   1. Contact tracing is verified locally, by the mobile applications themselves and not through the central server, the central server only keeps record of infected EphIDs for the other applications to check against. DP-3T keeps data local to devices where possible. It doesn’t require all applications to report back with their EphIDs, only infected user data (the random strings) gets uploaded publicly.
5. Strategy 5: Minimizing Replication
   1. No data relevant to the users (such as EphIDs) is replicated, not to mention that every EphID is unique, and replication could pose a risk of EphID conflicts.
6. Strategy 6: Minimizing Retention
   1. Data is kept on a need-be basis which in this case is the amount of time it would take for the “infectious period” to be over, which can vary. But all data is regularly rotated, and nothing is retained, any data that is not relevant is deleted.

**Sources**

* [ACLU White Paper — Principles for Technology-Assisted Contact-Tracing](https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing)
* [Decentralized Privacy-Preserving Proximity Tracing Wikipedia](https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing#cite_note-whitepaper-1)
* [DP-3T White Paper](https://raw.githubusercontent.com/DP-3T/documents/master/DP3T%20White%20Paper.pdf) (raw pdf from the [github](https://github.com/DP-3T) repo)
* [DP-3T comic](https://github.com/DP-3T/documents/blob/master/public_engagement/cartoon/en/comic-en.pdf)