Design Principles for Data Protection and Privacy:

- Only collect enough data to fulfill our stated purpose
- Where possible anonymize data.
    - Where that isn't fit for purpose, de-identify data.
    - Where anonymization and de-identification of data are not fit for purpose, psydonynomize data.
    - Never use personal identifiable information without robust encryption.
    - Only use encrypted personal identifiable information as a last resort when all other levels of anonymization, de-identification and psydonynomization have proven not fit for purpose.
- Complete pseudonymization and/or anonymization of personally identifiable information on edge devices before transmitting to across network connections.
- Commitment to open-sourcing the security and privacy relevant business logic of the system for public inspection.
- Employ an AI and data science ethics checklist directly in the codebase[1]
- Adhere to GDPR regulations and adhere to the Ethics Guidelines For Trustworthy Ai set forth by the European Commission.[2]

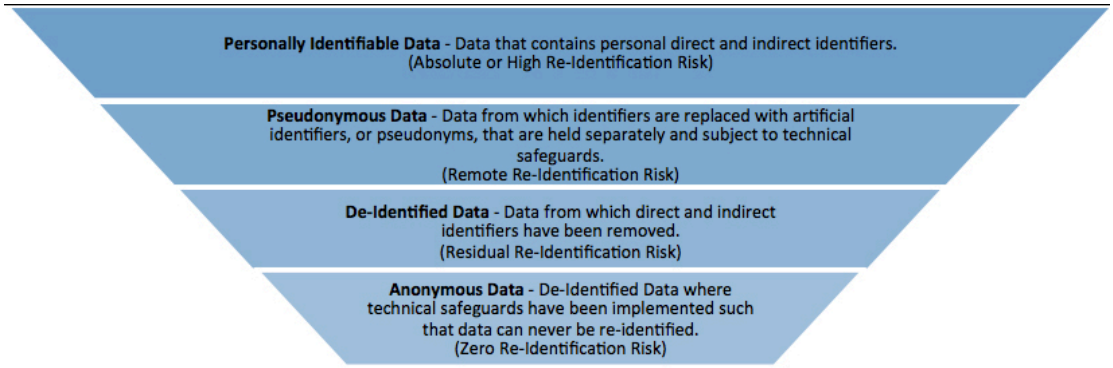
M-Zone Privacy controls

- Raw video cach/storage is temporary and only stored locally.
- Raw video processing on edge devices (not transmitted to offsite or cloud storage)
- Raw video cach/storage deleted automatically on a rolling basis
- Computer vision algorithm recognizes publicly available license plate numbers
- No facial or biometric recognition employed
- Following license plate recognition cached video is deleted
- License plate numbers will be processed using at a minimum pseudonymization techniques.
- Raw plate numbers will be deleted from edge devices following initial processing and will never be transmitted beyond the edge device (not transmitted to offsite or cloud storage)
- Strong cryptographic techniques will be employed to produce at a minimum a psydonynomous output on which autonomous economic agents can act and driver incentivization can be performed.
- Driver/visitor incentivization and the mapping of driver wallets to their psydonynomized plate identifier will the an OPT IN process.
- Driver/visitors may OPT OUT at any point and the mapping of between their driver wallets to their psydonynomized plate identifier will be irreversibly deleted throughout the system.

[1] https://deon.drivendata.org/#using-this-tool
[2] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

- Where feasible, cryptographic techniques will be utilized to harden psydonynomized data against various de-psydonynomization attacks. Psydonynomization will not be achieved through a naive use of a simple hashing algorithm such as SHA-256.
- When a partial pseudonym is sufficient to provide the stated functionality a partial pseudonym shall be utilized instead of a complete pseudonym to limit correlation attack vectors.
- When possible salt rotation shall be employed
- Decentralied system architecture to reduce or eliminate single points of failure
- Advanced cryptographic techniques such as Password-Based Key Derivation Function 2 (PBKDF2) or Bcrypt and salted hashing will be employed to protect against de-psydonynomization attacks such as rainbow table attacks and brute force cracking with a particular eye toward preventing attacks using ASIC, FPGA or Quantum computing techniques to de-psydonynomize user data in the future.

Glossary:



[3]

[3] https://www.bclplaw.com/en-US/insights/at-a-glance-de-identification-anonymization-and-pseudonymization-1.html