DATA SECURITY & PRIVACY - FAQ

1. What kind of data will be required to participate in the pilot program?

To <u>sign up</u> for the Voatz app, voters will need to provide the following:
   a) Valid email address
   b) Valid mobile number

To <u>get verified</u> as an eligible voter remotely, voters will need to scan the following inside the app:
   a) A government issued photo ID document
   b) A live selfie

Once voter identity and eligibility is fully verified, the ID scan and selfie are deleted (typically within 24-48 hours). This information is not used for any other purpose whatsoever. The identity verification process follows the NIST SP 800-63 guidelines.

2. How is the data kept secure and private?

State of the art encryption techniques, including end-to-end encryption, are used to secure data transmission as well as secure data storage. The pilot platform utilizes a highly resilient and tamper resistant blockchain based infrastructure. The security keys are distributed amongst multiple stakeholders (including jurisdiction staff members) so as to minimize the chances of any accidental data leakage or insider attacks. The platform runs on a FedRAMP certified cloud infrastructure.

3. What is the data sharing policy?

Personally identifiable information (PII) data about voters is only used for verifying voter eligibility during the duration of the pilot program and is never shared with any third parties for any other purpose (such as advertising, etc.). As stated above, the ID scan and live selfie are deleted within 24-48 hours of voter verification.

Voter email addresses and mobile numbers are used to deliver notifications, reminders, and receipts to voters during the duration of the pilot program and are not shared with any third parties for any purpose outside of this pilot program.

4. **How long is the data retained?**

   Once voter identity and eligibility is verified, the ID scan and selfie are deleted (within 24-48 hours in most cases). The Voatz app also offers voters the ability to exercise the '*right to be forgotten*' once the election is over in order to facilitate a complete account deletion (including email address and mobile number) if the voter so desires. Voters always have the option to sign up again for any future uses.

   Election data (such as the record that the voter has participated in the pilot, the printed paper ballot, etc) is retained as per the standard election data retention policies of the City of Chandler and the State of Arizona. After the standard data retention period, upon the authorization of the City Clerk, all traces of electoral data captured within the pilot system, including back-ups and summary data, can be returned to the city or fully destroyed subject to applicable laws. Any destruction of data by Voatz can be witnessed by person(s) appointed by the Clerk, and Voatz will issue a certificate of destruction signed by Voatz and the appointed witnesses.

5. **What is the likelihood of identity theft during the pilot program especially for technology challenged users?**

   The likelihood is extremely low. All data is transmitted and stored using state of the art encryption techniques. Once voter identity and eligibility is verified, the ID scan and selfie are deleted (within 24-48 hours in most cases). This minimizes the threat surface significantly - *if the data doesn't exist anymore then it can't be stolen or misused.*

   In addition, all pilot participants will be offered multiple training and orientation sessions (videos, online zoom, in-person at selected locations, etc.) that will include an overview of personal mobile security best practices. Phone and email support will also be available to assist voters in having a highly secure yet seamless pilot experience.