CITIZENS.IS

Your Priorities and data protection

Introduction

Your Priorities is operated by the non-profit Citizens Foundation Iceland, whose mission is to help increase trust in politics. Data privacy is a major focus of the organization; this commitment is manifested in the many different privacy-related features that are part of Your Priorities.

Key data privacy principles

- **Collect as little personal data as possible**
  - Collection of personal data is by default limited to name, email address (to maintain contact with users about issues they are interested in), password and an optional profile image
  - Users can then generate and submit content in the form of text, audio and video
- **Allow users to be anonymous to others if they so choose**
  - Users can use a nickname instead of their real name
  - Groups can also be setup to allow completely anonymous logins that do not require entering any personal information
- **Users are clearly informed about how data is used and processed**
  - Community operators create a privacy notice that is prominently accessible through a link when the user first signs up and is also available through the question mark link, displayed at the top of the application at all times
- **Users can easily view, delete and anonymize data they have submitted**
  - When deleting their accounts users are presented with the options of either delete or anonymize all their data
  - After anonymization of data nothing in Your Priorities will connect the user personally to that data
  - The user is in full control of their own data
- **Citizens Foundation never shares or sells any personal data**
  - As a non-profit there is no pressure to monetize data via 3rd parties

Data security infrastructure

The Your Priorities application is hosted on the Heroku application deployment platform in two separate locations in Ireland and the USA on Amazon AWS. The Citizens Foundation chose

Heroku as its application hosting partner partly because of their advanced and comprehensive security solutions.

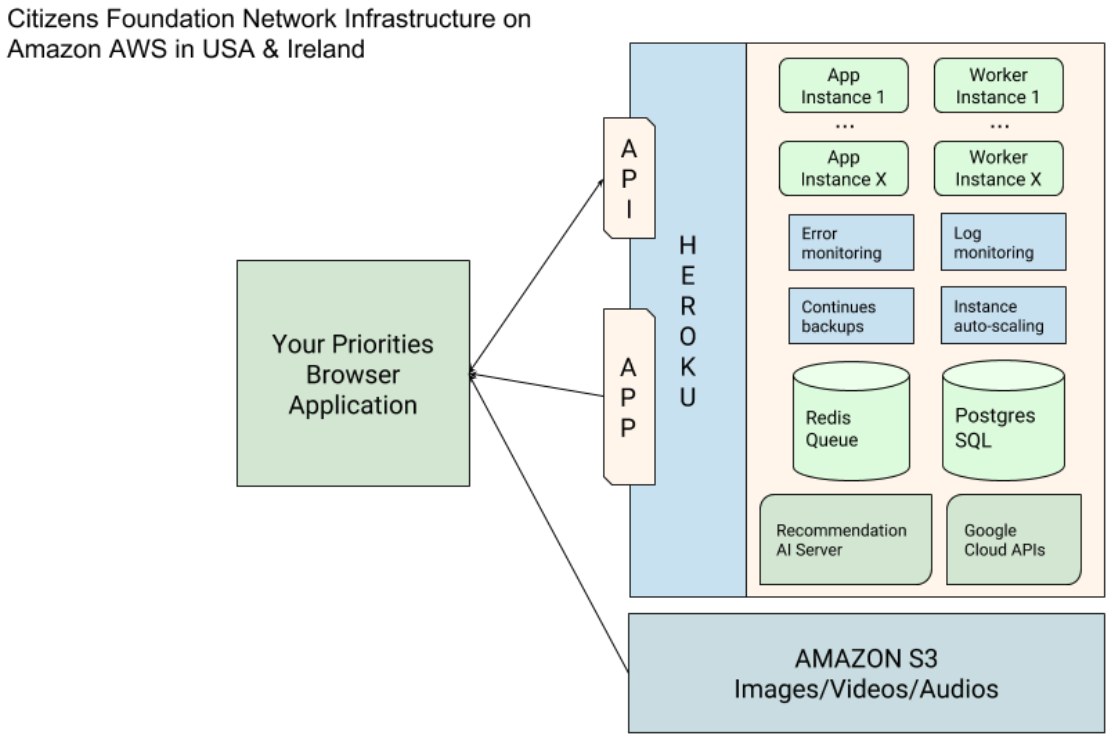
Here are some of the key elements related to data security:

- **Heroku (Salesforce) and AWS security teams manage all platform security & infrastructure**
    - Provides state-of-the-art software and physical data security with the following certifications
        - ISO 27001
        - SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
        - PCI Level 1
        - FISMA Moderate
    - Citizens Foundation only has access to deploy the Your Priorities application, to view log files, to access data on the website and to download backups of data
    - Citizens Foundation has no access to any underlying infrastructure
- **Data is always transported encrypted**
    - When data is accessed from the website to administrators browsers
    - When the app web instances communicate with the database
    - During continuous database backups
    - When transferring weekly “physical” backups to the Citizens Foundation offices in Reykjavik
- **Google Analytics (optional as Plausible is now built in on the Your Priorities backend)**
    - Is the only analytics service enabled by default
        - Facebook Pixel can also be used but is disabled by default
    - IP addresses are explicitly anonymized before they go into Google Analytics
        - More information on how this works here: https://support.google.com/analytics/answer/2763052?hl=en
    - Only a limited number of Citizens Foundation employees have access to the Google Analytics reporting interface
- **Other Google Cloud Services**
    - Your Priorities uses the following Google Cloud APIs: Google Translate, Google SpeechToText and Perspective API
    - All data is encrypted while communicating with those APIs and no data is stored on Google Cloud, those service are only used for transient processing of data
- **Passwords**
    - Passwords are stored encrypted in the database
- **Cookies and tracking**
    - Your Priorities does not track users with cookies
    - Your Priorities only uses temporary session cookies with no tracking ability
    - Google Analytics cookies

        - No personal information is sent to Google Analytics
        - IP addresses are anonymized (see above)
        - Advertisement features and 3rd party sharing are turned off in Google Analytics so there is no tracking enabled there
    - As there is no tracking, no cookie tracking consent is needed on Your Priorities websites
- **Limited access to personal data**
    - Only a limited number of Citizens Foundation technical employees have access to databases that include personal data
        - All have signed a declaration of confidentiality
        - List of current Citizens Foundation employees with access is available on request
        - New employees at Citizens Foundation will not get access to databases with personal data until proven to be reliable
    - Operators of communities on Your Priorities are also required to limit administration access to personal data
    - Data from different Citizens Foundation partners is stored in a SQL database with secure access protocols

CITIZENS.IS

Technical overview:
The Citizens Foundation runs two completely separate Heroku/SalesForce app clusters, one in the United States and one in Ireland.



More information on:
Heroku Security infrastructure is here: https://www.heroku.com/policy/security. On data protection in general: https://devcenter.heroku.com/articles/security-privacy-compliance And on GDPR specifically: https://devcenter.heroku.com/articles/gdpr

AWS security infrastructure is here: https://aws.amazon.com/security/ And AWS GDPR related information is here: https://aws.amazon.com/compliance/gdpr-center/

Google Cloud security infrastructure is here: https://cloud.google.com/security/ And information related to GDPR specifically https://cloud.google.com/security/gdpr/

CITIZENS.IS

Operators with communities on the yrpri.org & ypus.org domains

- **In regards to GDPR then operators of communities on yrpri.org are either:**
  - **Joint controllers with the Citizens Foundation which is also a data processor**
    - Service Level Agreement between the operator and Citizens Foundation covers all GDPR issues
  - **Citizens Foundation is the sole controller and data processor**
    - Service Level Agreement between the operator and Citizens Foundation covers all GDPR issues
- **Operators of communities are required to include their own privacy terms explaining how they will use and process the data**
  - Privacy terms can be authored with the Pages feature in Your Priorities and a “Page” can be selected in Community Edit to be displayed prominently as a link when the user registers for the first time. This is a simple and transparent way of informing the user about how the data will be used and processed. The privacy policy is also available under the question mark at the top of the screen in the app
- **Operators of communities on Your Priorities have full access to all data except passwords**
  - All data can be easily deleted or anonymized
    - If an operator decides to anonymize data this will happen with a 7 day delay and the user will receive an email and be able to delete their data before it is anonymized, if they so choose
  - Operators are encouraged to include a section in the privacy notice about data retention. In many cases, for the types of communities on Your Priorities, the case can be made for storing the data “indefinitely” for historical purposes but the options to delete or anonymize the data after a certain period are also easy to execute in the Your Priorities administration interface

Operators with own domains on Your Priorities

- **Regarding GDPR, with domain level hosting, the domain owner is a sole controller and Citizens Foundation is a data processor**
  - GDPR related issues are covered in the legal service level agreement between the domain owner and the Citizens Foundation

- **The users are not exposed to neither the Your Priorities brand nor the Citizens Foundation brand as the service is provided on a strictly “white label” basis**
    - Example of domain level Your Priorities hosting is Better Reykjavík (https://betrireykjavik.is/) and the Scottsih Parliament (https://engage.parliament.scot/)
- **When an operator hosts on the domain level on Your Priorities there are no privacy or terms notices displayed to users from the Your Priorities platform or from the Citizens Foundation**
    - All terms and privacy notices come from the operator of the domain & communities
- **Emails will come from the operators domain and will be answered by the operator**
    - This Citizens Foundation provides 2nd line support for support related queries
- **Option to enable Facebook login with enhanced privacy protection that disables Facebook tracking of user activities**
- **Option to enable secure SAML based Single-Sign-On (SSO) as a login option**
    - In Iceland the government has a SSO solution called “island.is” that users can use to login to many government services. This secure Icelandic government login option is integrated with Your Priorities sites from in Iceland
    - When users login using an external SAML based SSO solutions no password is stored in the Your Priorities database
    - Only one SAML based SSO solution can currently be used per domain

Key data related processes

- **Backups**
    - The Heroku platform provides continuous rolling backups that have the option of rolling back the database to any date within 2 weeks or download a snapshot from any given date in that period
    - Physical backups are downloaded by employees of the Citizens Foundation every week and stored in a highly encrypted digital vault in the Citizens Foundation office in Reykjavík that is protected by a security system
    - Operators of domain & communities on Your Priorities are encouraged to set in place their own backup strategies for their data
- **Data retention**
    - Continuous platform backups are stored for 2 weeks on a rolling basis
    - Detailed platform log files are stored for 4 weeks on a rolling basis
    - Physical off-site backups in Reykjavík are stored for 12 months and then destroyed
- **Data protection related questions or issues**

    - Citizens Foundation Data Protection Officer is Robert Bjarnason, robert@citizens.is and he is responsible for the following:
        - Point of contact with both users and data protection authorities
        - Monitor all data protection efforts and policies
        - Train staff members that have access to personal data
        - Evaluate data protection methods and processes regularly

Data breach policy

In the unlikely event of a data-breach, where personal data is stolen, the following key steps will be executed:

- Affected 3rd party operators and users will be notified no later than 2 working days after the breach is discovered and users encouraged to change their passwords
- Investigation will be started immediately, with security partners
    - Make sure that the breach is not ongoing and stop it if it is
    - Identify the vulnerabilities that led to the breach and fix them
    - Inform 3rd party operators and users about exactly what happened and how it was fixed

The Citizens Foundation has been operating digital democracy platforms for over 14 years and no data breach of any kind has happened since we started.