Plan Overview

A Data Management Plan created using DMPonline

Title: Familia Sicura Tecnology Venture Plan

Creator:JUAN UNRIZA

Principal Investigator: Vittorio Loreto, JUAN CALRLOS UNRIZA VARGAS

Data Manager: Vittorio Loreto

Project Administrator: JUAN CALRLOS UNRIZA VARGAS

Affiliation: Sapienza University of Rome

Template: DCC Template

Project abstract:

Nowadays, there is a huge gap between the accelerated evolution of technology and the living conditions of the global population. Especially, in the recent years, the worldwide elderly population has been affected by the cybercrime dramatically, cybercrimes focus on fraudulent schemes executed online via email, SMS, or social media to steal money or personal data as known as "scam", against seniors has reached a crisis point. According to the last report from The Global Anti-Scam Alliance –GASA (GASA, 2025), worldwide losses have increased by 400% in the last 5 years, and in 2025 have been estimated to $442 billion dollars.

In Italy, that trend is significantly accelerating into 2025, the economic and financial cybercrime remains a key issue, with 27,085 cases handled and 4,489 people investigated, according to the Polizia Postale Italian. As a respond strategy, they have been working on Digital Inclusion for elderly populations, with projects such as "Cyber Security for All", emphasizing their role in prevention and education, promoting awareness-raising, (Stato, 2026). Additionally to this situation, the European Union Agency For Cybersecurity –ENISA (ENISA, 2025), in their report

2025 has confirmed that traditional cybersecurity solutions, such as conventional antivirus software have limited utility against next generation AI-driven threats or even the social engineering based, due to, the antivirus operates by detecting malicious code, but the social engineering or Deepfake have not any kind of that code.

Finally, the silver economy sector will be hardly able to prevent those crimes and improve their safe digital environment. The Italian silver generation requires a familiar community empowered with the skills to protect itself, thereby increasing its digital resilience. For those concerns, we created "Familia Segura" to offer a solution through protection services delivered directly to Italian familiar units, through a "Family Digital" platform, it is specifically designed to help to improve their security by their own members.

ID: 204439

Start date: 23-02-2026

End date: 31-05-2026

Last modified: 15-05-2026

Copyright information:

Familia Sicura Tecnology Venture Plan

Data Collection

What data will you collect or create?

For the design and validation of the business case, the project gathers data from the following sources:

- Primary Institutional Sources (Italy):
  - ACN (Agenzia per la Cybersicurezza Nazionale): Real-time bulletins on voice-cloning threats.
  - Polizia Postale: Annual reports on cybercrime trends affecting elderly population in Italy.
  - ISTAT (Istituto Nazionale di Statistica): Demographic data on the Silver Economy and smartphone penetration among citizens aged 70+.
- Secondary & Global Sources:
  - Eurostat: Digital literacy and vulnerability statistics across the European Union.
  - Europol / Interpol: Global reports on "Grandparent Scams" and AI-driven social engineering trends.
  - PNRR (Piano Nazionale di Ripresa e Resilienza): Strategic indicators for digital resilience and innovation funding.

How will the data be collected or created?

Development data will be stored in open formats (CSV, JSON, WAV) to ensure reproducibility in research labs.

Documentation and Metadata

What documentation and metadata will accompany the data?

Metadata Standard: The DCAT2 vocabulary will be used to track the lineage of testing datasets (https://www.w3.org/TR/vocab-dcat-2/).

Ethics and Legal Compliance

How will you manage any ethical issues?

No real private calls will be used during the development phase; only simulated or consented datasets. In any cases, each activity would be checked to comply with the Euopean Union's General Data

Protection Regulation GDPR, and all metadata collected for R&D purposes will be pseudonymized at the source.

How will you manage copyright and Intellectual Property Rights (IPR) issues?

Data derived from institutional partnerships (ACN/Polizia) will be handled according to strict non-disclosure agreements (NDAs).

Storage and Backup

How will the data be stored and backed up during the research?

Develop environment: data will be hosted in a GDPR-Compliant Cloud Hub (Italy/EU based) to ensure data sovereignty.
Preservability: Key research findings and anonymized validation datasets will be preserved in repository Ricerc@Sapienza https://research.uniroma1.it/node/48

How will you manage access and security?

The access of the repository Ricerc@Sapienza https://research.uniroma1.it/node/48 is manage by the IT Sapienza area. At Sapienza University of Rome, the Role-Based Access Control RBAC principles are applied to secure university portals, manage student privacy, and organize research data by ensuring only authorized users access specific systems

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved?

In the cases that transcription of the consented calls will be preserved by 10 years. The decision if and how. other datasets are to be shared and/or archived will be made on a case-by-case basis.

What is the long-term preservation plan for the dataset?

The data will remain on the repository Ricerc@Sapienza https://research.uniroma1.it/node/48, with access remaining to data owners that were previously defined.

Data Sharing

How will you share the data?

During the project phases all data will be shared between the members of the project. However, at the end of the project most of the data will be shared in the repository Ricerc@Sapienza https://research.uniroma1.it/node/48.

Are any restrictions on data sharing required?

Due to the datasources there is no restrictions on data sharing, except the transcription of the possible consented calls, those are only able to be shared as pseudonymized data.

Responsibilities and Resources

Who will be responsible for data management?

Chief Data Officer (CDO): Juan Carlos Unriza Vargas

What resources will you require to deliver your plan?

Access and permissions for the repository Ricerc@Sapienza https://research.uniroma1.it/node/48.