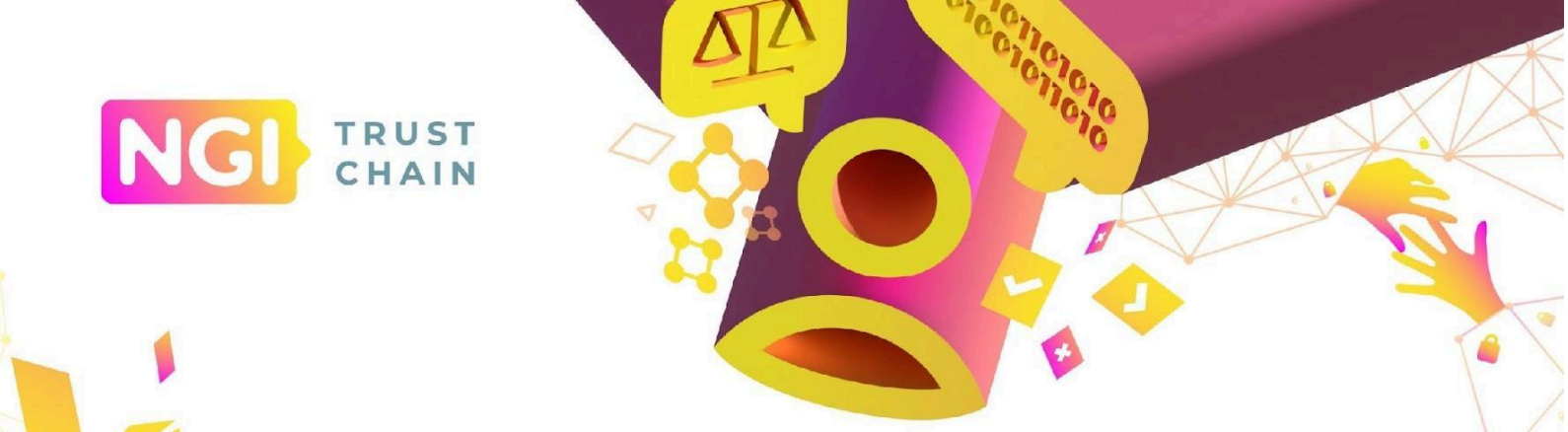

D4. Modularized Software Components Ready for Distribution, Full Documentation for Developers/Users, Final Business Plan, and Result of the Validation process

IM4DEC

04/04/2024 (submission date)

Funded by the European Union

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Grant Agreement No.: 101093274
Call: HORIZON-CL4-2022-HUMAN-01
Topic: HORIZON-CL4-2022-HUMAN-01-03
Type of action: RIA

D4. Modularized Software Components Ready for Distribution, Full Documentation for Developers/Users, Final Business Plan, and Result of the Validation process

>IM4DEC<

Due date	04/04/2024
Submission date	04/04/2024
Deliverable lead	OwnYourData
Version	1.0
Authors	Christoph Fabianek (OwnYourData), Jan Lindquist (OwnYourData)

Executive Summary

UN convention Article 9 requires countries to take measures for the full and equal participation of persons with disabilities, including access to communication and information services. Despite this, there are still about 1 million deaf and hard of hearing persons in Europe who currently rely on outdated technology (e.g., fax) and help from others to make an emergency call.

DEC112 is a non-profit association that has designed and developed a standard-conform infrastructure (ETSI TS 103 479) for deaf emergency chats (ETSI TS 103 698). Since 2019, the association is operating a system in Austria in collaboration with the Ministry of Interior that connects emergency chats to the appropriate emergency communication centre by utilising location information.

However, still a number of challenges exist that are addressed in the NGI TRUSTCHAIN funded project "IM4DEC - Identity Management for the Digital Emergency Call":

- Presenting a verified identity when delivering an emergency chat: extend current SMS verification with an eIDAS or eIDAS 2.0 compliant identity based on DIDs
- Operators struggle with chats from deaf persons: introduce an AI-based chatbot to train users and share this information with emergency organisations as basis for new training material
- Such data (identity, emergency information, training chats) are considered special category data under the GDPR and we will perform a formal DPIA (Data Protection Impact Assessment) for the end-to-end dataflow

The above goals are not only for the benefit of deaf people but also individuals oppressed by domestic violence can make use of this technology through the use of a silent emergency notification; already in operation since 2022 in Austria we will provide an SDK to include this functionality in an EU Digital Identity Wallet to get such functionality on every smartphone.

Finally, EU Authorities addressed these topics in Regulation 2023/444 that require all member states to ensure accessible communication services to emergency services from 2025 onwards: With our initiative we want to make sure that such future solutions take special needs of the deaf community and oppressed individuals into consideration.

Funded by the European Union

Table of Contents

Funded by the European Union

List of Figures

Funded by the European Union

List of Tables

Funded by the European Union

ABBREVIATIONS

ARF	Architecture and Reference Framework (for EUDI wallets)
API	Application Programming Interface
BCF	Border Control Function
CAD	Computer Aided Dispatch
CHE	Call Handling Equipment
CPE	Call Processing Equipment
D2A	Domain specific Data Agreement
D3A	Domain specific Data Disclosure Agreement
DEC	Digital Emergency Communication (previously: Digital Emergency Call)
DID	Decentralised Identifier
DIF	Decentralised Identity Foundation
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DRI	Decentralised Resource Identifier
ECC	Emergency Control Center
ECRF	Emergency Call Routing Function
ESInet	Emergency Services IP Network
ESRP	Emergency Service Routing Proxy as defined in ETSI TS 103 479
ETSI	European Telecommunications Standards Institute
EUDI	European Union Digital Identity
GPT	Generative Pre-trained Transformer
HTTP	Hypertext Transfer Protocol
ID	Identity
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
LIS	Location Information Service

Funded by the European Union

LoST	Location-to-Service Translation
NG	Next Generation (in Europe: NG112, in the US: NG911)
OIDC	OpenID Connect
OID4VCI	OpenID for Verifiable Credential Issuance
OYD	OwnYourData
OYDID	Own Your Decentralised Identifier (`did:oyd` method)
PSAP	Public Safety Answering Point
PSQL	PostgreSQL (Relational Database Management System)
REST	REpresentational State Transfer
RDF	Resource Description Framework
SIP	Session Initiation Protocol
SHACL	Shape Constraints Language
SMS	Short Messaging Service
SOyA	Semantic Overlay Architecture
SSI	Self-Sovereign Identity
TLS	Transport Layer Security
VC	Verifiable Credential
VP	Verifiable Presentation
W3C	World Wide Web Consortium
YAML	Yet Another Markup Language

1 Introduction

The overarching goal of the IM4DEC project is to spearhead a significant leap forward in the domain of Decentralised Identifiers (DIDs) by introducing the concept of DID Rotation. This innovative approach not only seeks to implement DID Rotation but also strives to establish a robust framework for standardisation and validation within the DID Resolution process. By doing so, we aim to address crucial challenges related to digital identity management, security, and privacy.

In addition to the technical aspects, the project places significant emphasis on the legal foundation for the widespread adoption of DIDs. This includes the development of a comprehensive Data Protection Impact Assessment (DPIA), which will ensure that the implementation of DIDs in the emergency services domain complies with all relevant data protection and privacy regulations. This legal framework will not only protect individuals' rights but also foster trust and confidence in the use of DIDs.

Furthermore, this project is firmly rooted in the context of emergency services, a domain where the stakes are particularly high. By integrating DIDs into the emergency services sector, we are taking concrete steps towards supporting marginalised communities and those who have been oppressed. This endeavour will enhance the accessibility and responsiveness of emergency services, making them more equitable and inclusive for all, regardless of their background or circumstances.

In summary, this project represents a multifaceted effort to improve digital identity management through the introduction of DID Rotation, while simultaneously addressing the legal and ethical dimensions of this technology. By situating these developments within the crucial domain of emergency services, we aspire to create a safer, more equitable, and more accessible world for everyone.

Funded by the European Union

2 Final Software Code and Documentation

This section provides a comprehensive view of the developed software, establishing a tangible record of our project's outcomes and serving as a guidepost for future research and development.

2.1 Project Repositories

This section outlines the various code repositories and data storage locations used throughout the project.It provides clarity on the projects access protocols, and version control systems in place, ensuring a transparent and efficient management of project resources.

Repository Name	Link	Kind	Restrictions
oydid	https://github.com/OwnYourData/oydid https://www.npmjs.com/package/oydid	public	none
didlint	https://github.com/OwnYourData/didlint	public	none
soya	https://github.com/OwnYourData/soya https://www.npmjs.com/package/soya-cli	public	none
ssi-mobile-wallet	https://github.com/OwnYourData/ssi-mobile-wallet	public	none
veramo	https://github.com/OwnYourData/veramo	public	none
RegAPI	https://github.com/dec112/dc-reg-api	public	none
RegAPI - SMS Plugin	https://github.com/dec112/dc-reg-sms	public	none
RegAPI - ID Austria Plugin	https://github.com/dec112/dc-reg-ida	public	none

Repository Name	Link	Kind	Restrictions
RegAPI - SIP Plugin	https://github.com/dec112/dc-reg-sip	public	none
DEC Onboarding	https://github.com/OwnYourData/dc-dec_onboarding	public	none
DEC112 SDK	https://github.com/dec112/ng112-js https://www.npmjs.com/package/ng112-js	public	none
Chatbot	https://github.com/OwnYourData/dc-chatbot	public	none
Data Intermediary	https://github.com/OwnYourData/dc-intermediary	public	none

Table 2.1: Project Repositories

2.2 Full Software Documentation

In Deliverable D3 we have described how to compile, deploy, and test our solution. This section is a short documentation about the functionality.

2.2.1 DEC112 Onboarding with ID Austria

To provide a verified identity in the DEC112 app (available on Android and iOS), the existing DEC112 registration element (Registration API) was updated to support the onboarding process using an existing eIDAS identity provider (in Austria the eIDAS conform "Bürgerkarte" and "Handy Signatur", and now the already available "ID Austria'' will develop into an eIDAS 2.0 compliant identity provider).

Upon receiving a verified identity (using OIDC, Authorization Code Flow), SIP credentials are created in the SIP Service and stored on the DEC112 app so that emergency chats can be initiated.

2.2.2 Triggering a Silent Emergency Notification from the Sphereon Wallet

To give as many people as possible access to emergency services, DEC112 and the Austrian Ministry of the Interior extended its services in April 2022 to offer a "Silent

Emergency Notification": either in situations when you cannot talk (e.g., shooting in a bank) or also for individuals oppressed by domestic violence. Especially, for domestic violence the challenge is to have an unobtrusive app, such that an aggressor does not remove the app from the victims smartphone.

In this use case we use a government issued identity (ID Austria) with OwnYourData acting as issuer for a Verifiable Credential that holds this government issued identity together with personal data (name, date of birth, and registered primary residence address). Based on this identity, SIP credentials are created and also added to the Verifiable Credential. The Verifiable Credential is added to an EU Digital Identity Wallet (we are using the wallet from Sphereon[1] but it should work with any standard-conform EUDI wallet) and through the DEC112 SDK a silent emergency notification can be triggered from within the wallet.

2.2.3 ChatGPT based Chatbot and Data Sharing

On the other end of an emergency chat is an operator in a control room that needs to be specifically trained on how to handle text-based emergency communication. With the advent of AI-based chatbots (e.g., ChatGPT) we want to provide functionality to simulate a control room operator and enable all DEC112 users to test emergency chats without requiring a human operator. Those chats can be - upon consent - shared with emergency service providers to increase the available training material for operators.

The whole process of collecting and sharing chat data is ensured to be GDPR compliant through a Data Protection Impact Assessment and using Data Agreements to document the data exchange.

2.2.4 DID Rotation

DID Rotation refers to the process of changing (or “rotating”) the underlying DID method for a given Decentralised Identifier. The concept is rooted in the best practices of cryptographic key rotation, where keys are changed periodically to reduce the risk of compromise. In the same way, periodically rotating a DID could reduce the risks associated with a specific DID method. And of course it avoids a lock-in situation into a given DID method.

[1] https://sphereon.com/sphereon-products/sphereon-wallet/

Rotating a DID method involves a number of steps and Figure 2.5 depicts our approach that transforms an original DID `v1` into a new DID `v2'`. In this process it is necessary to take a number of precautions to ensure complete evidence when updating the DID method.

One specific challenge when performing a DID rotation is to ensure full compliance of both DID methods with relevant properties of the DID Core Specification[2]. To validate those properties the OwnYourData DID Lint service[3] will be extended with checks in the DID metadata and the resolution process. Only DID methods compliant with these checks are possible candidates for DID rotation. As a first step, we will demonstrate DID rotation from the `did:oyd` to the `did:ebsi` method.

[2] https://www.w3.org/TR/did-core/
[3] https://didlint.ownyourdata.eu/

3 Demonstration and Exploitation

3.1 Solution Demonstration

The following video was recorded to demonstrate the IM4DEC solution:

https://youtu.be/3tauhBTEjsk

3.2 Communication, Dissemination, Exploitation Results

This section focuses on the strategies and outcomes associated with sharing our research findings and the developed software product with relevant stakeholders and the wider community.

The following blog posts were created during the course of the project:

- OwnYourData Blog: Project Start
  https://www.ownyourdata.eu/en/ngi-trustchain-funding-for-im4dec/
- OwnYourData Blog: DID Rotation
  https://www.ownyourdata.eu/en/did-rotation/

IM4DEC was mentioned on Social Media in the following posts/tweets:

- Project Start
  https://x.com/NGI_TRUSTCHAIN/status/1679806285624012800?s=20
- NGI TRUSTCHAIN Interview:
  https://x.com/NGI_TRUSTCHAIN/status/1768200394197323993
- NGI TRUSTCHAIN Promotion:
  https://www.linkedin.com/posts/ngi-trustchain_digitalidentity-decentralization-trustchain-activity-7173966129927766016-aXFT
- DID Rotation:
  https://www.linkedin.com/feed/update/urn:li:activity:7150075552593330176
  https://www.linkedin.com/posts/cheqd-identity_did-activity-7176163986294370304-wk6y
  https://twitter.com/OwnYourDataEU/status/1744308724582207529
  https://twitter.com/cheqd_io/status/1770396571298890180

Collaboration on standards development on DID Rotation in the DID Registration Specification:

- Github of Decentralized Identity Foundation:
  https://github.com/decentralized-identity/did-registration/pull/32

List of exhibitions the team of OwnYourData and DEC112 plan to attend:

- EENA Conference 2024 - https://eenaconference.org/
  presentation of IM4DEC project results on Thursday April 25th, 2024 on main stage at 9am together with representatives of Apple and Google on the topic of "Transmitting medical data from the phone to PSAPs"; conference program: https://eenaconference.org/wp-content/uploads/2023/12/2023_12_06_EENA-2024_Programme_Overview-2.pdf

4 Technical Value Added

4.1 Key Innovations of the Solution

Our research project has delivered relevant advancements in digital identity, security, and interactive training platforms, marking significant strides in technological integration and user engagement. Below are the key innovations of our solution:

Government-Issued Digital Identity with ID Austria

At the heart of our solution is the integration of ID Austria, a government-issued digital identification system. This innovation provides users with a secure and reliable form of identification that can be used within DEC112. By leveraging ID Austria, we ensure that our solution meets the highest standards of identity verification and security, facilitating trust and compliance in digital transactions.

Integration into the Registration API Component

The integration of ID Austria into the Registration API component enables an efficient and streamlined user registration process. It allows for real-time verification of user identities during the registration phase, significantly reducing fraud and ensuring that only verified users gain access. The seamless nature of this integration enhances user experience while maintaining strict security protocols.

Management of `did:oyd` in Sphereon Wallet

The project introduces an innovative approach to use decentralised identifiers (DIDs) by utilising the Sphereon Wallet for silent emergency notifications. This approach not only provides users with control over their personal data but also enhances security and privacy. Through the Sphereon Wallet, users can manage their digital identities without relying on centralised authorities, paving the way for a more decentralised and user-centric digital ecosystem.

Technical Viability Demonstrated Through DIDs, VCs, VPs, OID4VCI

Our solution demonstrates technical viability through the use of Decentralised Identifiers (DIDs), Verifiable Credentials (VCs), Verifiable Presentations (VPs), and the OID4VCI framework. This combination ensures a robust and secure framework for digital identities, enabling users to share verified credentials without compromising their privacy. The use of these technologies showcases our commitment to

leveraging cutting-edge solutions to enhance digital security and user autonomy.

Demonstration of DID Rotation

A key feature of our solution is the demonstration of DID Rotation, which allows users to change their DID without losing their digital identity or credentials. This feature is crucial for avoiding lock-in to a specific DID method, ensuring that users retain flexibility and control over their digital identities. DID Rotation exemplifies our solution's adaptability and forward-thinking approach to digital identity management.

ChatGPT-based Chatbot for Emergency Situation Training

Our solution incorporates a ChatGPT-based chatbot designed to train users in emergency situations, yielding very positive results from user feedback. This innovative use of AI provides a safe and interactive platform for users to learn and practice handling various emergency scenarios. The chatbot's ability to simulate realistic interactions and provide immediate feedback has proven to be an effective tool for emergency preparedness.

Legally Conform Sharing of Chatbot Conversations with Authorities

In addition to its training capabilities, our solution also demonstrates the ability to share chatbot conversations with authorities in a legally conform manner. This feature ensures that valuable insights and data generated during emergency situation training can be shared with relevant authorities, enhancing collaboration and response strategies. The careful consideration of legal conformity in this process underscores our commitment to privacy, security, and compliance in digital communications.

Overall, our solution represents a significant leap forward in digital identity management, emergency training, and secure data sharing. By harnessing the power of ID Austria, innovative DID management, cutting-edge technologies, and AI-driven training tools, we have developed a comprehensive and user-centric solution that showcases the importance and viability of SSI (self-sovereign identity) in digital innovation.

4.2 Suggested Evolutions for the Solution

Our research project has achieved significat progress in enhancing digital identity management, emergency response training, and secure, flexible data sharing. However, the landscape of digital innovation is continually evolving, necessitating ongoing improvements and adaptations. Below, we outline the suggested evolutions for our solution, focusing on three key areas: ID Austria integration, the Chatbot, and DID Rotation.

ID Austria Integration Enhancements

- Voluntary Inclusion of Additional Information: While not making ID Austria mandatory in the registration process, we suggest evolving the system to encourage users to voluntarily include additional information. This approach enhances user profiles without compromising the ease of use or privacy, thereby enriching the user experience and security.
- Support for Web-Flow and In-App Flow with Fallback Option: To accommodate diverse user preferences and technological accessibilities, integrating support for both web-flow and in-app flow is essential. A fallback option will ensure uninterrupted service, catering to all user scenarios and enhancing overall accessibility.
- Timeline Information Provision: Implementing the features to provide control rooms with clear timelines regarding the validity and renewal dates of the provided registration information can significantly improve compliance. This transparency ensures call takers are always aware of the provided information status, reducing the risk of potentially outdated information.
- Regular Update Reminders: To maintain the accuracy of user information, integrating a system to trigger reminders for users to regularly update their registration details is crucial.

Chatbot Evolution

- Diverse Personalities: Introducing chatbot personalities, such as Marvin and Mother Theresa, can create a more engaging and fun chat experience. By varying the chatbot's tone and interaction style, users can enjoy a more varied experience.
- Collaboration with Emergency Response Centres: Enhancing the chatbot's effectiveness involves collaborating with emergency response centres to improve the quality of questions and mimic actual emergency flows. This collaboration ensures the chatbot's scenarios and responses are grounded in real-world emergency protocols, enhancing the training's effectiveness.
- Improved Handling of Medical Conditions: It is critical to refine the chatbot's

ability to handle certain medical conditions to avoid wrong recommendations. This involves integrating additional information and expert knowledge in the system prompt to ensure accurate guidance for all users.

- Continuous Data Exchange with DEC112 and Emergency Response Organizations: Establishing a framework for continuous data exchange between DEC112 and emergency response organisations can provide mutual insights from ongoing chatbot tests. This collaboration ensures that the chatbot evolves based on real-world data and feedback, enhancing its accuracy and reliability.

DID Rotation Advancements

- Integration into UniResolver.io: Collaborating with DanubeTech to integrate DID Rotation into UniResolver is a key step and already ongoing. This enables all conforming DID methods to support DID Rotation seamlessly, ensuring users can maintain control over their digital identities without being locked into a specific DID method.
- Implement "DID Rotate" Functionality in UniRegistrar.io: To further ease the process of DID Rotation, implementing a "DID rotate" functionality directly in Uniregistrar.io is suggested. This native support for DID Rotation across all DID methods simplifies the user experience, making it straightforward for users to maintain their digital autonomy.

These suggested evolutions aim to refine and expand the capabilities of our solution developed so far in the course of NGI TRUSTCHAIN OC1. It will ensure that it remains adaptable, user-friendly, and at the cutting edge of technological advancements.

4.3 Present or Future Patentability of the Solution

In the world of software development, the issue of patentability, particularly in the realm of open-source software, presents a complex debate. Open source software is typically characterised by a commitment to communal collaboration and unrestricted access. It is designed to be freely available for anyone to use, modify, and distribute. By its very nature, open source software contrasts with the idea of patenting, which involves granting exclusive rights to an invention or solution for a specific time frame. Patenting tends to be more compatible with proprietary software, where restrictions on use, modification, and distribution can be more readily implemented.

While it is technically possible to patent certain aspects of open-source software if

they meet the criteria for patentability, doing so can often be at odds with the open-source philosophy. For us, choosing not to patent the developed open-source solution aligns with the broader academic and research ethos, fostering a climate of collaboration and shared progress. Such a decision also aids in facilitating wider adoption and utility of the software, further supporting innovation and advancement in the respective field.

Even within the framework of open-source software, it's important to note that there can still be room for patenting under certain circumstances. For example, our solution could potentially be patented within a very specific, defined use case (e.g., some supply chain niche markets.) This scenario would entail identifying a unique application of the software, demonstrating its novelty, non-obviousness, and utility, which are the general criteria for patentability. While the broader software code might remain open for use and modification by others, the patent would protect this specific implementation or application, preventing others from commercially exploiting it without permission.

5 Business Model and Exploitation Plan (Final)

This is the final version of our business model and exploitation plan for the IM4DEC project. This section extends the content provided in D3.

5.1 Business Model Description

The Digital Emergency Communication Association has been diligently working on offering an effective solution for deaf individuals to enable them to engage in emergency chats. The service, as detailed on https://DEC112.at, addresses the need for accessible communication in emergencies, ensuring safety and inclusivity. With EU Regulation 2023/444 coming into effect, our business model is well positioned to fill a critical gap in emergency services.

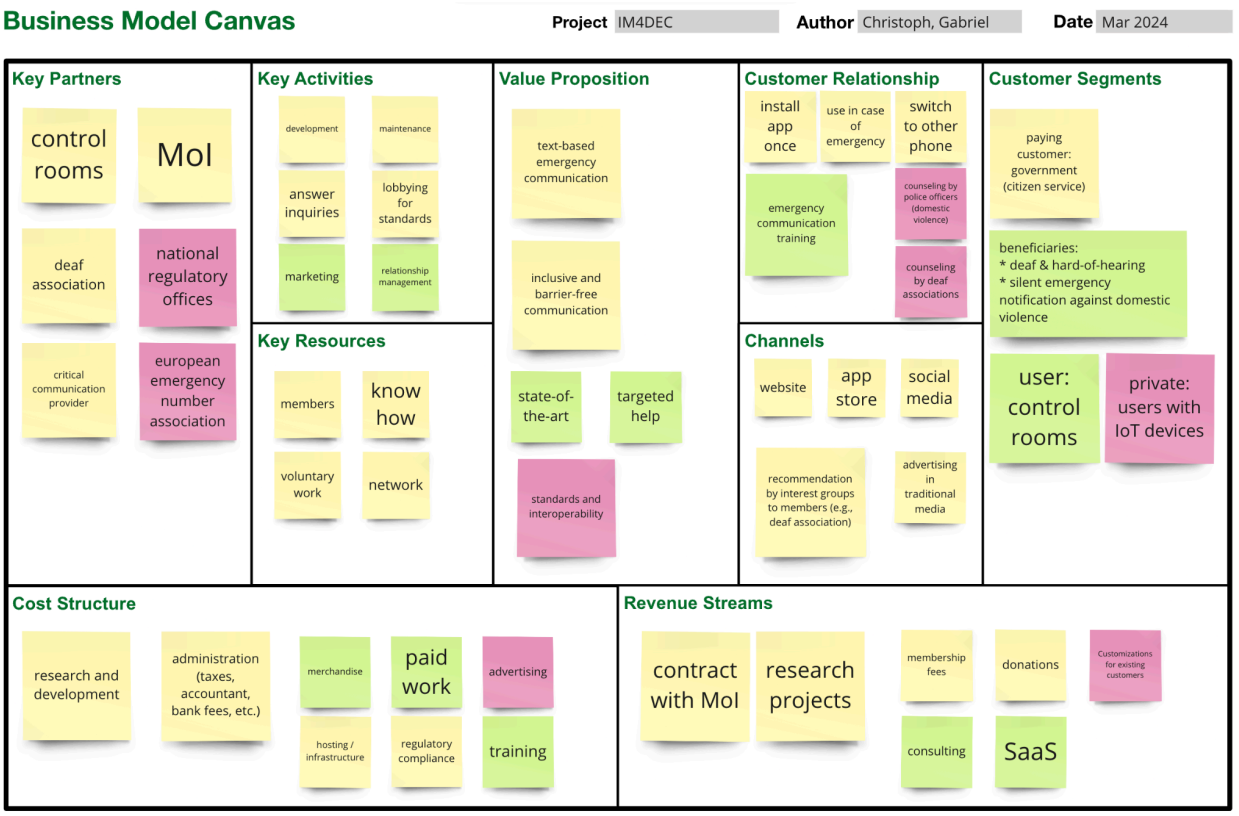

Figure 5.1: Business Model Canvas

The Business Model Canvas depicted in Figure 5.1 is the result of multiple team

sessions to provide a comprehensive few of the business aspects of DEC112. Specifically we discussed cost and revenue streams and the remainder of the chapter provides a more detailed elaboration.

Below are the most relevant cost streams in our business model:

- Research and Development: to ensure that the service continually meets the needs of its users
- Infrastructure Maintenance: to maintain the servers, databases, and ensure the chat system's uptime
- Training & Outreach: to educate emergency service providers and the deaf community about the functionality and benefits of the platform
- Regulatory Compliance: ensuring the chat system is compliant with the EU Regulation 2023/444 and other pertinent regulations

These are the primary revenue streams:

- Licensing: partnering with emergency service providers and charging a licensing fee for integration into their systems
- Partnerships: partnering with device manufacturers to integrate our system directly, offering them a compliant solution
- Grants & Donations: as a solution catering to a specific community, there are opportunities for funding through grants and donations

5.2 Economic Analysis

Focusing on potential customers, our service targets a niche yet vital segment: around 1.8 million individuals who are deaf or are hearing impaired in Austria. However, the scope of our service transcends this group, extending to all Austrians who might find themselves in situations where a silent or text-based emergency call is necessary. This broadens our potential customer base significantly, encompassing the entire Austrian population.

When considering competitors, the landscape in Austria appears moderately competitive. There are a few organisations offering similar services (app-based emergency calling), but their number is limited to single digits. Furthermore, all competitors are just collecting additional data to an emergency, while still calling the emergency number via traditional phone call, whereas DEC112, in contrast, uses a multimedia IP infrastructure to forward emergency calls. This also allows for a direct integration of services into the respective emergency response centres, where DEC112 has already 6 control rooms connected, serving all 9 federal countries and covers fire, ambulance, police and mountain rescue services.

Regarding the role of partners we already have or anticipate forging alliances with a variety of entities, including emergency response centres, associations like the Deaf Association of Austria, and key organisations such as the Federal Ministry of the

Interior (BMI) and the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR). These partnerships will not only extend our reach but also enhance our credibility and operational efficiency. Combined with the fact of being a non-profit association, driven by innovation and not profit, DEC112 has already grown to an established entity in the Austrian landscape of emergency calling.

5.3 Business Value for the Blockchain and SSI Domain in General

The integration of Blockchain and SSI (Self-Sovereign Identity) offers enhanced security, transparency, and user control in emergency communication. Using decentralised systems, our platform can ensure user privacy and data integrity. Furthermore, as Blockchain and SSI continue to gain traction across various sectors, we start now to integrate our emergency communication with other platforms to create a cohesive, interoperable ecosystem, ensuring efficient and secure emergency communication.

As a very concrete contribution to the SSI domain, a collaboration between OwnYourData and the UniResolver was initiated in the course of the project to provide DID Rotation for all DID methods. Through initial discussion in the DIF WG-ID bi-weekly calls it was agreed that an adapted resolution process for DID Rotation should be implemented right in the UniResolver.

5.4 Business Value and Relevance for TRUSTCHAIN

What is the link between your business and TRUSTCHAIN?

TRUSTCHAIN focuses on creating decentralised, transparent, and user-friendly digital services. Our emergency chat system can leverage TRUSTCHAIN's services to ensure that the communications between the help-seeking individual and the emergency services are secure, transparent, and incorruptible. The ongoing project evaluates the trustworthiness and dependability of other TRUSTCHAIN services that might be integrated.

As a first tangible result an integration with the Sphereon Wallet was implemented and demonstrated: Users with a DEC112 Credential are now enabled to trigger a Silent Emergency Notification from the login screen.

What would the value exchange be?

For TRUSTCHAIN, partnering with our solution provides a real-world use case, demonstrating its versatility and applicability in emergency services. It further strengthens TRUSTCHAINs position as a leader in the domain. In return, our platform benefits from the network and available know-how of the TRUSTCHAIN community.

5.5 Any Other Impact

This section discusses societal, environmental, legal and policy impacts.

Societal: Our solution serves as a trailblazer for inclusive tech, showcasing how technology can be harnessed to cater to specific communities, which in our case are people with disabilities and people suffering from domestic violenceFurthermore our technology facilitates the freedom of choice, which DID provider one may choose. With DIDs being a fundamental part of a person's identity, it's crucial that this identity is not bound to a single provider and can be freely migrated to other providers.

Environmental: By digitising emergency communication, we reduce the need for physical resources and logistics traditionally required for assisting the deaf community, contributing to a reduced carbon footprint.

Legal & Policies: With the EU Regulation 2023/444, our solution not only meets a regulatory need but also empowers the deaf community, offering them autonomy in emergency situations and promoting inclusivity.

In conclusion, our business model and exploitation plan solidly place us at the intersection of open technology, accessibility, and emergency services. As we move forward, our commitment remains to ensure safety and inclusivity for all.

6 Pilot Studies Results

This chapter presents a comprehensive overview of the outcomes derived from our pilot studies, serving as a pivotal component of our project. The emphasis here is on providing background and motivation as well as data collected, alongside the feedback received from users who interacted with our solution. Our intent is to delineate not only the quantitative and qualitative results but also to highlight the significance of these findings in demonstrating the effectiveness and impact of the solution we propose.

6.1 Brief account of all the co-creation process

In the co-creation process for enhancing our emergency call application, several critical requirements were identified to address the system's existing challenges and to harness technology for improved service quality. Firstly, **enhancing the onboarding process** was prioritised to ensure control centre operators have immediate access to comprehensive caller information, enabling a more personalised and efficient response during emergencies. Secondly, the introduction of a **robust identity verification system** was deemed essential to mitigate misuse and maintain service integrity, ensuring resources are appropriately allocated and potentially recovering costs in abuse cases. A shift away from the monolithic architecture of the current system was also identified as crucial. This **move towards a modular design** aims to simplify maintenance, expedite feature deployment, and enhance overall system resilience. Additionally, recognizing the infrequent user interaction with the DEC112 app, there was a consensus on the need for an **improved chatbot**, and providing a more intuitive and user-friendly test environment. Lastly, **evaluating Kubernetes** for modernising the hosting solution was highlighted as a strategic initiative. This evaluation is aimed at leveraging advanced cloud-native technologies for better deployment, management, and scalability of the application, aligning with modern software development best practices.

In the project, our approach was methodically structured and executed in phases, beginning with the internal definition of the desired target architecture within the OwnYourData & DEC112 team. This initial step was crucial, as it laid the foundation for the subsequent development and implementation processes. By establishing a clear vision for the target architecture, the team could align on the technical and functional specifications needed to achieve the project's goals. This comprehensive planning phase ensured that the solution not only met the current requirements but also had the flexibility and scalability to adapt to future needs.

Following the architectural planning, the project moved into the implementation phase, characterised by active engagement and dialogue with a diverse group of stakeholders. These discussions included representatives from the Ministry of the Interior, regulatory authorities, control rooms, medical professionals, and social workers, ensuring that the solution addressed the wide range of needs and concerns of those directly and indirectly impacted by the project. In addition to stakeholder consultations, the project team conducted extensive testing with selected users, including individuals with disabilities, public safety workers, acquaintances, and anyone interested through publicly available information who wanted to try the ID Austria and chatbot features. This inclusive testing strategy was pivotal in gathering valuable feedback, identifying usability issues, and refining the solution to better serve all user groups, demonstrating a commitment to inclusivity and user-centric design.

The culmination of the co-creation process was marked by a comprehensive evaluation encompassing several key aspects, ensuring the project met its objectives with high standards of quality and effectiveness. Technically, the project underwent a detailed assessment of the infrastructure used and the quality of implementation, scrutinising the robustness, security, and scalability of the solution. The applicability of ID Austria was specifically evaluated, confirming its integration and functionality within the ecosystem, which was crucial for streamlining the registration process and enhancing user verification. The new registration process's overall suitability was also assessed, ensuring it was user-friendly and efficient. The quality of chatbot conversations was rigorously analysed, focusing on their relevance, user engagement, and ability to provide accurate and helpful responses. Additionally, the project's success was measured through the quantitative tracking of predefined KPIs, capturing user satisfaction and operational efficiency of the solution. The documentation of these results within this document serves not only as a testament to the project's achievements but also as a valuable resource for future initiatives, providing insights and learnings that can inform and guide subsequent developments.

6.2 Validation Plan

At DEC112, having a well-defined strategy is essential for the successful introduction of new components into production. Our validation plan is comprehensive, incorporating both qualitative and quantitative metrics to monitor our objectives effectively. This approach is guided by our primary mission to protect the integrity and security of the critical safety environment where our solutions operate. By doing

Funded by the European Union

so, we commit to maintaining the highest standards of safety and performance across our deployments.

General steps to put new components into production:

1. Local implementation based on agreed requirements and design
2. Implementation of tests and documentation of deployment requirements
3. Staging Meeting (announced on DEC112 Slack on #general channel)
4. Deployment on staging environment (information on Slack when complete)
5. Monitoring of tests and KPIs (incl. documentation of any changes in system)
6. Production Meeting (announced on DEC112 Slack on #general channel)
7. Deployment on production environment
8. continuous monitoring of the new component(s) through established processes

During the evaluation period on the staging environment (step 5) we conducted thorough validation sessions involving a diverse range of participants to ensure comprehensive feedback and insights. In January, we initiated interviews with key stakeholders, including representatives from the Ministry of the Interior, regulatory authorities, control rooms, medical professionals, and social workers. These discussions were aimed at gathering expert opinions and requirements to refine our solution's design and functionality. Following this, in February, we expanded our validation efforts to include user tests with selected individuals. This group comprised persons with disabilities, public safety professionals, an extended network of acquaintances, and anyone interested in testing the ID Austria and chatbot functionalities, as informed through publicly available information. These sessions were crucial for assessing the usability and accessibility of our solution, ensuring it met the diverse needs and expectations of all potential users, thereby validating the effectiveness and user-friendliness of our proposed enhancements.

For the purpose of this research project our goals of user engagement for each component is detailed below. The numbers were determined to be statistically significant to draw valid conclusions, while also being manageable in terms of data collection and analysis.

- Registration API: 50 users
- Wallet: 15 users
- Chatbot: 200 conversations from at least 50 users
- DID Enhancements: 15 users

The application of our criteria and KPIs has culminated in clear recommendations for the further development and productive deployment of our solution. These insights, derived from rigorous analysis and validation sessions, have paved the way for strategic enhancements and optimizations. In the following section, we will delve into these recommendations in greater detail, outlining specific actions and improvements that will ensure our solution not only meets but exceeds the expectations and needs of our users. This structured approach towards continuous

improvement highlights our commitment to delivering a robust, efficient, and user-centric solution, setting a solid foundation for its success in the real-world environment

6.3 Status of Validation

We are pleased to report that the validation process has been successfully completed, providing us with the essential information required for the productive deployment of our solution. This milestone marks a significant achievement in our project's lifecycle, as it confirms the readiness of our solution to transition from the development phase to real-world application. Based on the outcomes of our comprehensive testing, the following list outlines learnings and specific measures that can be implemented to further enhance our solution.

ID Austria

- the integration should be offered as optional additional information after SMS registration (to automatically fill out the current form in the app to provide personal information); too many errors (by users as well as erroneous behaviour of ID Austria) make this form of registration not yet suitable as primary onboarding variant
- ID Austria information should be displayed in the course of an emergency call as verified information with a timestamp when the ID Austria registration was performed (might be already outdated)
- both registration flows (in-app and web flow) should be provided for registration
- using the in-app flow for registration is more convenient but does not go through in about 1/3 of the cases for unexplained reasons
- web flow registration requires several steps but is stable (and provides more information for debugging)
- Google initially flagged the redirect page after the ID Austria page as a possible phishing site; After we reported it as a valid site, this warning no longer occurred

Registration API

- modular structure with Redis has proven to be stable and easy to administer
- traceability of individual user registrations is detailed, but at the same time GDPR issues of the privacy analysis (see Appendix B) can be successfully addressed

- for easier debugging, a timestamp of the creation of a data set and a timestamp for the last change to the data set should also be stored in the hashmaps in Redis

Silent Emergency Notification

- switching to another app was initially not recognized and resulted in confusing responses from ChatGPT (has already been fixed)
- repeated questions about the address or repeated information about dispatching forces were addressed by changing the configuration
- concerns were mentioned by expert users (who work in control rooms) that the questions in general make sense but a real emergency call has another tone and different vibes
- some medical questions discussed were bizarre (but could have stemmed from the curiosity of our subjects)

Chatbot

- the feature with the countdown when the emergency call is triggered was positively received by users and it was recommended to also adopt this UI element in the DEC112 app
- the button to trigger the silent emergency call is too small

Overall System Setup

- the monitoring for the test system should be at the same level as the productive system in order to detect crashes of individual components more quickly
- for Kubernetes, the individual nodes must have sufficient memory (at least 4GB, better 8GB) for stable operation -> that didn't work well on test system 1 (had only 2GB), but it did work well on test system 2 (8 GB per node)
- the pre-reserved persistent volume of 200MB for the database was too small (the initial size of a PostgreSQL instance is over 8MB and 10+ databases are already created for the individual components without any data) -> it is better to reserve 500MB

In the validation phase, we have successfully achieved or even surpassed the following key performance indicators (KPIs). Below we describe the quantitative KPIs, split by the two test systems we evaluated.

Registration API

- plan: 50 users
- result:
  - test system 1: 55 (based on new DIDs created)
  - test system 2: 68 (actual users from log analysis)
- comment: the ratio of ID Austria registrations vs SMS registrations was 20% ID Austria vs 80% SMS; just over 1/3 of the users tried ID Austria, but only 1/5 were able to successfully complete the registration with ID Austria

Wallet

- plan: 15 users
- result: 17 users
- comment: only guided testing with face-to-face interaction with users took place; from today's perspective, productive use will still take more than 2 years

Chatbot

- plan: 200 conversations
- result:
  - test system 1: 36 conversations
  - test system 2: 146 conversations
- comment: an incorrect configuration on test system 1 made much of the test data inaccessible, but enough valuable insights were still collected to enable productive use; overall, more than 200 conversations were collected in the 9 months project duration
  the quantitative analysis of questions to participants after using the chatbot lead to the following results:
  - overall rating of chatbot interaction (1-bad to 10-good)
    - test system 1: 7,8
    - test system 2: 6.6
      all users except one very active user gave ratings between 5-10 but this very user gave 1 most of the time as response
  - consent to sharing the data with others (yes/no question)
    - test system 1: 21%
    - test system 2: 35%
  - provide contact method (email) for follow-up questions:
    - test system 1: 5%
    - test system 2: 12%

DID Enhancements (DID Rotation)

- plan: 15 users

- result: about 20 users were reached via DIF WG-ID calls in the form of presentations and conversations
- comment: the great success lies in the additional implementation of DID Rotation did:cheqd and the planned integration into the Uniresolver

7 Impact Assessment

A critical evaluation of the project's impact, including technological, socio-economic, and environmental aspects. This assessment reflects how the project contributes to TrustChain's objectives and KPIs.

7.1 Key Performance Indicators

This section evaluates the project against KPIs defined in the TRUSTCHAIN Deliverable 3.7 “TrustChain Support to third parties - Guide for implementation v1.0” in section 2.5.4

KPIs towards a more trustworthy and privacy-aware evolution of the internet

#	KPI	Project Contribution
1.1	Which is the Trust Assessment Effectiveness, e.g., accuracy for labelling/inference of the trustworthiness subjects or for content, for your solution.	trustworthiness is key for delivering emergency calls and by using a government issued ID for onboarding we improve the overall trustworthiness of the system
1.2	How can you assess the privacy/anonymity of your solution? E.g., employing probabilistic metrics, anonymity set size, entropy, etc.	a Privacy Report (Appendix A) and a Data Protection Impact Assessment (Appendix B) was performed
1.3	Security guarantees on trustworthiness/privacy, e.g., security proofs.	the project scope did not encompass dedicated security proofing, although it is being undertaken by a team with over 10 years of experience in safety-critical emergency communication
1.4	Did you employ/ implement zero knowledge proof protocols?	was not in project scope / is not implemented
1.5	How does your solution improve security and privacy, compared with existing solutions?	through the focus on established standards (ETSI TS 103 479 and ETSI TS 103 698) along the technical delivery of an emergency call, using the latest

#	KPI	Project Contribution
		established technologies (ID Austria, state-ot-the-art encryption standards), and performing a Privacy Report (Appendix A) and a Data Protection Impact Assessment (Appendix B) we ensure the highest level of security and privacy currently available for text-based emergency communication for the deaf and hard-of-hearing community

Table 7.1: KPIs towards a more trustworthy and privacy-aware evolution of the internet

KPIs towards a more decentralised NGI

#	KPI	Project Contribution
2.1	Did you implement new decentralised computing technologies for storing and accessing data, e.g., via the OAI-PMH protocol, that achieve high reliability, availability, Quality of Service, and similar properties necessary to realise new decentralised services?	was not in project scope / is not implemented
2.2	Did you implement new decentralised social networks?	was not in project scope / is not implemented
2.3	Did you implement new decentralised publishing platforms?	was not in project scope / is not implemented
2.4	Did you implement new Digital Twin technologies that can help establish digital representation of the reality in specific circumstances where needed?	was not in project scope / is not implemented

#	KPI	Project Contribution
2.5	How does your solution improve decentralisation, and how does that impact user experience, compared to existing solutions?	through the introduction of DIDs in the onboarding process for DEC112 services users are enabled to switch between service provider and are empowered to maintain their identity without relying on a third party; this even extends to the fact of switching DID providers through DID Rotation regarding user experience, a significant improvement in onboarding time is achieved by using ID Austria instead of SMS verification
2.6	Have you investigated the scalability of your decentralised solution?	The DEC112 app has now more than 32.500 users (as of Mar 2024) and design patterns as well as the components can easily handle a 10x increase in terms of users and call volume Due to thorough 24/7 (automated) end-to-end tests currently a call volume of 500.000 emergency calls is processed per year.

Table 7.2: KPIs towards a more decentralised NGI

KPIs towards sustainable business

#	KPI	Project Contribution
3.1	Market penetration potential? #of pilot users, # of potential customers, # of competitors, # of partners, etc.	Pilot users addressed in chapter 6.2 Validation Plan and other KPIs in chapter 5 Business Model and Exploitation Plan
3.2	Business model defined? Details should be mentioned, such as # of Business Use Cases (BUCs), # of BM canvases, # of BUCs analysed	addressed in chapter 5 Business Model and Exploitation Plan

#	KPI	Project Contribution
3.3	Profitability, e.g., ROI, NPV, payback period, etc.	only partially applicable since DEC112 and OwnYourData are non-profit organisations; relevant aspects addressed in chapter 5 Business Model and Exploitation Plan
3.4	Crypto strategy? Token type? Crypto distribution?	not applicable for IM4DEC

Table 7.3: KPIs towards sustainable business

KPIs towards new forms of human-centred interaction and immersive environments for NGI users

#	KPI	Project Contribution
4.1	Task Success rate. % of participants that successfully complete a task.	addressed in chapter 6 Pilot Studies Results
4.2	User Adoption Rate. How many new users does the tool have? What percentage represents the new users?	at the begin of the project DEC112 had about 20.000 registered users; as of Mar 6, 2024 there are now more than 32.500 users → this is an increase of >60%
4.3	User Satisfaction. How satisfied are the users with the solution? What is the % of satisfaction?	addressed in chapter 6 Pilot Studies Results
4.4	User error rate. How frequently users make mistakes during a specific task? Where do the users face difficulties with the product?	addressed in chapter 6 Pilot Studies Results
4.5	Time on task. How much time is the total learning time spent by the user to know how to use the solution?	no metrics are collected for time on task

#	KPI	Project Contribution
4.6	Navigation vs. search What the users prefer to do? Is the navigation process clear? How often do the users use the search function?	not applicable for the DEC112 solution
4.7	System Usability Scale (SUS) questionnaire. How usable is your solution for the users? Net Promoter Score. What is the % of likelihood that the users recommend the solution?	neither System Usability Scale nor Net Promoter Score were evaluated for the DEC112 solution

Table 7.4: KPIs towards new forms of human-centred interaction and immersive environments for NGI users

KPIs related to the pilot studies

#	KPI	Project Contribution
5.1	User Experience (UEQ questionnaire)	addressed in chapter 6 Pilot Studies Results
5.2	# of pilot users	addressed in chapter 6.2 Validation Plan
5.3	User Engagement (# of transactions per user, freq. of use, etc.)	addressed in chapter 6 Pilot Studies Results
5.4	# of interested users in future business collaboration	addressed in chapter 6 Pilot Studies Results; active collaboration with two other TRUSTCHAIN OC1 projects: DanubeTech and Sphereon
5.5	# of paying users	only partially applicable because this is a free service paid by the government; existing paid contract in Austria with Ministry of the Interior

#	KPI	Project Contribution
5.6	List of use cases in the pilot	use cases described in chapter 2 Final Software Code and Documentation
5.7	User story: List of actions accomplished by users to complete the different use cases.	addressed in chapter 6 Pilot Studies Results

Table 7.5: KPIs related to the pilot studies

Interoperability and standardisation

#	KPI	Project Contribution
6.1	Did you propose or could/will propose standards/drafts?	DEC112 is built on existing standards (specifically ETSI TS 103 479 and ETSI TS 103 698); in the course of the project we did not propose new standards
6.2	Describe international events on standardisation activities participated/contributed	invitation to present project results at the EENA 2024 conference in Valencia - the leading international conference hosted by European Emergency Number Association
6.3	What digital identity standards do you focus on?	W3C DID Core Spec v1.0
6.4	What standards related to credentials do you focus on?	W3C Verifiable Credentials Data Model v2.0
6.5	Which Blockchain network(s) and Smart Contract language(s), did you use?	the project aims to provide non-blockchain based solutions due to the performed DPIA for sensitive personal data handled in the course of emergency communication; for DID Rotation EBSI (European Blockchain Service Infrastructure) and did:cheqd was used

#	KPI	Project Contribution
6.6	Interoperability standards employed (syntactic interoperability)? Ontologies employed (semantic interoperability)?	Semantic Overlay Architecture (SOyA) used for syntactic interoperability; Ontologies employed: - SOyA Ontology (OWL) - DID Ontology (OWL) - SOyA DID Ontology (OWL, SHACL)
6.7	What interoperable data formats or communication protocols were used if any in the implementation?	interoperable data formats: - Data Agreements (ISO 27560) - PIDF-LO (RFC 5491) - LoST (RFC 5222) communication protocols: - ETSI TS 103 479 - ETSI TS 103 698 - SIP (RFC 3261)
6.8	Importance of interoperability in your solution? E.g., # of cross-chain transactions?	interoperability for DID methods was demonstrated through DID Rotation; interoperability for emergency communication through adhering to ETSI standards → both forms of interoperability are crucial for wider adoption

Table 7.6: Interoperability and standardisation

Legal and ethical compliance

#	KPI	Project Contribution
7.1	All users are informed about the processing of their personal data. An information notice has been put in place.	yes, information is available online (https://www.dec112.at/en/privacy-idaustria/)
7.2	Users' consent is asked and stored whenever consent is the relevant legal basis to be used.	yes, users give consent during the registration process and specifically for data sharing in chatbot conversations

#	KPI	Project Contribution
7.3	The purposes for processing personal data have been well-defined, specified and are communicated to the users and no personal data is processed beyond what is needed for these purposes.	yes, also a DPIA was performed (documented in Appendix B)
7.4	Retention periods for users' personal data are well-defined and are communicated to the users.	yes, as part of the privacy statement on the website (https://www.dec112.at/en/privacy-idaustria/) retention period is 3 month
7.5	Personal data are kept accurate, complete and up to date.	yes, this is also in the self-interest of the user when actually performing emergency communication
7.6	The necessary technical measures are taken to protect the personal data processed. Personal data are encrypted in transfer and at rest, where appropriate.	yes, and documented in a Privacy Report (Appendix A) and a detailed Privacy Analysis for ChatGPT (Appendix C)
7.7	All processors engaged provide adequate assurances and guarantees as required and the appropriate data processing agreements have been completed and signed.	yes, evaluated in the Privacy Report (Appendix A)
7.8	The processes are put in place to ensure compliance with data subject rights (e.g., right of access, correction, erasure, limitation, opposition, etc.).	yes, documented in a Privacy Report (Appendix A)
7.9	Personal data are only transferred to third countries to the extent that adequate protection can be foreseen.	personal data is not transferred to third countries in the current setting; with data agreements dedicated consent for sharing data with third countries is possible

#	KPI	Project Contribution
7.10	A record of processing activities is drawn up for the project and kept up to date.	yes, the processing activities are described in the DEC112 DPIA Report (Appendix B); the system keeps a timestamped log of all processing activities
7.11	The necessary approvals and authorizations from the competent ethics and/or governmental bodies for the processing of personal data are sought and obtained.	yes, this is covered in the established contract with the Ministry of Interior Austria

Table 7.7: Legal and ethical compliance

KPIs towards a greener NGI

#	KPI	Project Contribution
8.1	Carbon footprint, e.g., greenhouse gas emissions comparing with existing solutions	through avoiding the use of blockchain a reduction in carbon footprint is achieved
8.2	Consumption of energy	the solution is hosted on a managed Kubernetes cluster; we requested a statement of energy consumption from the hosting company but only got a general statement about the use of 100% green electricity
8.3	Supply chain miles	not applicable for the provisioning of emergency communication services
8.4	Saving life, improving biodiversity	during 2023 the DEC112 service delivered 1.500 emergency calls
8.5	Waste reduction and recycling rates	not applicable for the provisioning of emergency communication services

#	KPI	Project Contribution
8.6	Sustainable outcomes in economic, energy and/or the societal terms achieved	providing emergency communication services for the deaf community and people experiencing domestic violence is in line with the ESG goals and specifically the social aspects
8.7	Environmental sustainability standards and policies, e.g., Green Energy Generation Initiatives, Sustainable Development Goals	not applicable for the provisioning of emergency communication services
8.8	Addressing climate change? (yes/no)	not applicable for the provisioning of emergency communication services

Table 7.8: KPIs towards a greener NGI

KPIs towards innovation

#	KPI	Project Contribution
9.1	Did you implement new innovative TRUSTCHAIN use cases?	yes, all use cases are described in chapter 2
9.2	Did you implement new innovative TRUSTCHAIN reasoning technologies?	was not in project scope / is not implemented
9.3	Did you make any inventions in the framework of your project, in terms of patents, copyrights, design rights, trademarks, trade secrets, etc?	no, was not in project scope
9.4	Which are the most disruptive technology components of your solution?	DID Rotation as described in section 2.4

Table 7.9: KPIs towards innovation

KPIs related to the implementation

#	KPI	Project Contribution
10.1	Code simplicity (analyser used and results)	current standards in software development were adhered to but due to the complexity of components in different languages and heterogeneity in the overall solution dedicated code analysis for the overall solution was not performed (the software operates in a safety critical environment since 2019 and is monitored by the Austrian government)
10.2	Testability Coverage (method/tool used for testing and results)	for Ruby SimpleCov is used in the oydid gem, test coverage is 73%

Table 7.10: KPIs related to the implementation

7.2 TrustChain Specific Objectives

SO1- Empowering citizens, civil society and organisations to better govern their online data thanks to a human centric approach
fulfilled: our solution for digital emergency communication enables citizens, civil society, and organisations to take control of their online data, ensuring accessibility and privacy for individuals who are deaf or unable to speak, thus fostering an inclusive and empowered digital society
SO2- Ensuring individuals self-sovereign identity and virtual identity management
fulfilled: our solution leverages Decentralised Identifiers (DIDs) and incorporates ID Austria through Verifiable Credentials, allowing individuals to manage their identity with full sovereignty

SO4- Ensuring trust on the Internet and empowering citizen with online democratic organisation and mechanisms
fulfilled: by implementing state-of-the-art technology in compliance with current standards (ETSI TS 103 479, ETSI TS 103 698, W3C DID and Verifiable Credentials), our solution enhances trustworthiness and empowers citizens through secure and transparent mechanisms, enabling reliable participation in emergency communication
SO5- Developing new business and sustainable models for data sharing and online services exchange based on decentralised technologies and open source
fulfilled: developing and demonstrating DID Rotation in the course of the project will lead to the convergence of DID methods; this innovation underpins new, sustainable business models for data sharing and online service exchanges, leveraging decentralised technologies and open-source frameworks to ensure interoperability and security
SO8- Building and sustaining a European ecosystem of top Internet innovators, setting the course of the Internet evolution according to a human-centric approach.
fulfilled: our initiative extends digital emergency communication with DIDs, aligning with the upcoming eIDAS2 regulation and leveraging ID Austria; this strategy not only builds and sustains a European ecosystem of innovators but also steers the evolution of the internet towards a human-centric approach, ensuring secure and inclusive digital environments

Table 7.11: TrustChain Specific Objectives

8 Conclusion and Future Directions

In conclusion, our research project has demonstrated significant progress and transformative contributions to the fields of emergency response and digital identity. We have successfully demonstrated the use of a government issued identity (ID Austria) in the onboarding process of the DEC112 app, the use of a European digital identity wallet (Sphereon Wallet) for silent emergency notifications, and benefits of generative AI through training modes for emergency communication.

Moving forward, we have identified key areas of evolution that hold great promise for the continuous enhancement of our research. The further development of the Registration API, continuous research on eIDAS2 legislation for the eventual use of EUDI wallets, and general availability for DID Rotation to avoid vendor lock-in for DID methods.

Through these proposed advancements, we intend to continue breaking barriers and driving innovation in the digital landscape. We believe our research will play a significant role in shaping the future of digital identity and data management in emergency response. We look forward to the next phase of our endeavour, confident in our ability to make meaningful contributions to these important areas.

Funded by the European Union

9 TrustChain Innovation and Impact Questionnaire

INNOVATION 1	
1. Title of the innovation	
Please enter a meaningful innovation title (between 20 and 200 characters, spaces included). *This field will be revealed to the public on the TRUSTCHAIN website.* ***Tip:** This field is key and needs to be strong and clear. If possible, use a '**for**' clause. Examples of **poor versus good innovation titles**:* *'Laser Design Platform' (poor) vs 'Improved semiconductor laser design platform for RWG (Ridge Wave Guide) laser"(good)* *'Novel Robot Arm' (poor) vs 'Dextrous robotic slave arm **for** high radiation environments' (good)* *'Biosensors for diagnosis' (poor) vs 'Biosensors capable of breath and saliva monitoring **for** heart failure diagnosis' (good)*	
Identity Management for Digital Emergency Communication	
2. Description of the innovation *Please describe the innovation. Use less than 500 characters, spaces included.* *This field will **NOT** be revealed to the TRUSTCHAIN website*	
The project implements and evaluates an important advancement for Decentralised Identifiers: DID Rotation together with relevant standardisation and validation for the DID Resolution process. Furthermore, it provides the technical (Registration Service) and legal (DPIA) basis for individuals to use DIDs. All of this embedded in the highly relevant emergency services domain to support minorities and the oppressed.	
3. This innovation is ...	
Under development	
Already developed but not yet being exploited	X
Being exploited	
4. Characterise the type of innovation *(choose one only)*	
Significantly improved product	
Significantly improved service (except consulting services)	
Significantly improved process	X
Significantly improved marketing method	

Significantly improved organisational method	
Consulting services	
New product	
New service (except consulting services)	
New process	
New marketing method	
New organisational method	
Other	
5. Level of Innovation: What is the level of innovation? *(choose one only)*	
Some distinct, probably minor, improvements over existing products	
Innovative but could be difficult to convert customers	
Obviously innovative and easily appreciated advantages to customer	X
Very innovative	
6. How will the innovation be exploited? *(choose one only)*	
Introduced as new to the market (commercial exploitation)	
Only deployed as new to the organisation/company (new internal processes implemented, etc.)	X
No exploitation planned	
If 'no exploitation planned' is selected, explain why not:	
The registration process with ID Austria is an update to the current registration process with SMS. The Chatbot is an extension to the current/simple echo bot.	

7. Indicate the step(s) in order to bring the innovation to (or closer to) the market

Answer the following grid only if the answer to the previous question is 'Introduced as new to the market' (choose only one answer per row)

	Done or ongoing	Planned	Not planned but needed or desirable	Not planned and not needed
Technology transfer	X			
A partner's research team and business units are both engaged in activities relating to this innovation	X			
Market study				X
Prototyping in laboratory environment	X			
Prototyping in real world environment	X			
Pilot, Demonstration or Testing activities	X			
Feasibility study		X		
Launch a start-up or spin-off				X
Licensing the innovation to a 3rd party				X
Complying with existing standards	X			
Contribution to standards	X			
Raise capital				X
Raise funding from public sources	X			
Business Plan	X			
Other (please specify)				

If 'Other' is selected, please specify what other steps have been done or planned for this innovation:

not applicable

8. Is there a clear 'owner' of the innovation in the consortium or multiple owners? *Only for multi-beneficiary projects*	
One clear owner	X
Multiple owners	

9. Indicate (up to a maximum of 3) key entity(ies) delivering this innovation.
DEC112 (www.dec112.at)
OwnYourData (www.ownyourdata.eu)

10. Indicate these entities' needs to fulfil their market potential			
	DEC112	OwnYourData	
Investor readiness training			
Investor introductions			
Biz plan development			
Expanding to more markets	X		
Legal advice (IPR or other)			
Mentoring or Coaching			
Partnership with other SME(s)		X	
Partnership with large corporates			
Incubation/Startup accelerator			
Executive Training			
Other			

11. For the entity chosen as one of the 3 'key innovators', will this innovation will be used by mainly current or new customers?	
Current customers	X
New customers	

12. Market maturity: The market targeted by this innovation is ... *(choose one only)*	
The market is not yet existing and it is not yet clear that the innovation has potential to create a new market	
Market-creating: The market is not yet existing but the innovation has clear potential to create a new market	
Emerging: There is a growing demand and few offerings are available	X
Mature: The market is already supplied with many products of the type proposed	
13. Market dynamics: is the market ... ? *Answer this question only if the answer to the previous question is 'mature'.*	
In decline	
Holding steady	X
Growing	
14. Are there other markets for this innovation that the innovators are not yet targeting?	
Yes	X
No	
15. Market competition: How strong is competition in the target market?	
Patchy, no major players	
Established competition but none with a proposition like the one under investigation	X
Several major players with strong competencies, infrastructure and offerings	
16. When do you expect that such innovation could be commercialised (from today)?	
Less than 1 year	
Between 1 and 3 years	
Between 3 and 5 years	X
Between 5 and 10 years	
More than 10 years	

17. Has a trade mark been registered for this innovation?	
Yes	X
No	
18. Which of the Societal Challenge(s) is/are the innovation relevant to?	
Health, demographic change and wellbeing	X
Food security, sustainable agriculture, marine and maritime, Bioeconomy	
Secure, clean and efficient energy	
Smart, green and integrated transport	
Climate action, environment, resource efficiency and raw materials	
Europe in a changing world - inclusive, innovative and reflective societies	
Secure societies - protecting freedom and security of Europe and its citizens	
Not relevant to any Societal Challenge	
If 'not relevant to any SC is selected' explain why?	
not applicable	
19. Which of the UN Sustainable Development Goals (SDGs) does this innovation contribute to?	
SDG 1 – No Poverty	
SDG 2 – Zero Hunger	
SDG 3 – Good Health and Well-being	X
SDG 4 – Quality Education	
SDG 5 – Gender Equality	
SDG 6 – Clean Water and Sanitation	
SDG 7 – Affordable and Clean Energy	
SDG 8 – Decent Work and Economic Growth	
SDG 9 – Industry, Innovation, and Infrastructure	
SDG 10 – Reducing Inequity	

SDG 11 – Sustainable Cities and Communities	
SDG 12 – Responsible Consumption and Production	
SDG 13 – Climate Action	
SDG 14 – Life Below Water	
SDG 15 – Life On Land	
SDG 16 – Peace, Justice, and Strong Institutions	
SDG 17 – Partnerships for the Goals	
Not relevant to any SDG	
If 'not relevant to any SDG is selected' explain why?	
not applicable	
20. Does this innovation have a potential to address climate mitigation or climate adaptation? *Climate mitigation potential: The innovation addresses the causes of climate change (i.e. it can reduce and curb greenhouse gas emissions)* *Climate adaptation potential: The innovation can reduce vulnerability to the harmful effects of climate change*	
Mitigation potential	
Not applicable for this innovation	X
Adaptation potential	

DEC112 Privacy Report

Assessment

Date: 2024-03-29

LINALTEC AB
Assessment by:
Jan Lindquist (GDPR Privacy Advisor)
jan@linaltec.com
+46 730 694 942

Funded by the European Union

History

2023-08-31 - initial Version

2023-10-20 - first update: minor changes in text to improve clarity, add references in Table A.1 to DEC112 JIRA ticketing system and current status of actions

2024-01-19 - second update: feedback from Ruben Roex (Timelex) incorporated. Added reference to EDPB as additional guidelines for performing DPIA.

2024-03-29 - final version: closed AP5, training performed. Reviewed new privacy policy for idaustria. Matomo as an analytics supplier and updated third party inventory list.

Executive Summary

This is an executive summary of the preliminary findings of the GDPR assessment of DEC112 association activities. This summary also covers the results of a DPIA assessment covered in a separate document

- A major vulnerability is registration API for new users and due to cleartext keys can be easily copied. Rate limitations should be in place to limit any potential attacks.
- Agreement between association and Ministry of Interior needs to be revised and association should have clear statements on what data can be transferred and historical data is discarded in case of disbanding the association.
- The DEC112 app needs a DPA with the association to make it clear the separation of responsibilities. The DEC112 app would be treated as an independent third-party.
- The usage of chatgpt should continuously be checked for any biases in chat simulations. Initial chat simulations look promising but need to be frequently checked if going live (simulation only).

Introduction

DEC112 association contracted Linaltec AB to perform a privacy assessment and provide a list of recommendations. Interviews were conducted with the following groups:

- Gabriel Unterholzer - chairman of the association as well as main developer, devops responsible.
- Mario Murrent - DEC112 app dev of mobile application and registration SDK
- Wolfgang Kampichler - standard responsible in ETSI and external partners, Ministry and political level

- Christian Fabianek - backend developer

This report is split into four areas: General Privacy Assessment, Routines, Data Breach Analysis and Systems Review. The General Privacy Assessment checks the risks surrounding the private data collected like cookie usage and privacy policy. The Routines section identifies the activities at DEC112 that handle personal information and need internal policies. The Data Break Analysis reviews IT related activities and potential data breach areas which raises the risk for GDPR penalties. The Systems Review checks for GDPR compliance of external systems and DEC112 association role in relation to these systems.

At the end of the report there is a summary of all the action points and recommended priority.

General Privacy Assessment

Risk Assessment

Companies need to assess the sensitivity of the data that is collected and determine if a threshold is reached where a larger risk assessment is required, this is called a Data Protection Impact Assessment (DPIA). A DPIA report identifies potential risks where top management decides the actions to mitigate any high-level risks.

To determine if a DPIA report is required a list of criteria are reviewed. If any of the criteria are yes, a DPIA should be conducted. Note this evaluation is only a guidance and each organisation may make their own decision to perform a DPIA.

Criteria for risk	Applicable?
1. Evaluation or scoring	No
2. Automated decision making	No
3. Systematic monitoring	No
4. Sensitive data	Yes (1)
5. Large scale data processing	No (2)
6. Datasets are matched/combined	No
7. Data relating vulnerable individual	Yes (4)
8. Innovation use of technology	Yes (3)
9. Prevents using a service or a contract	No

Note – For details on individual criteria refer to either EDPB[4] or ICO guidelines[5].

[4] EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determing whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

[5] ICO Guidelines for Data Protection Impact Assessments: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

DEC112 association is required to perform a DPIA due to the following reasons:

(1) Emergency chat sessions may include sensitive communication when using the app to inform health situations or personal injury. Additionally, Apple Health and Google Health data might be added to chat session which may include health conditions
(2) There are ~20k registered users in the app. This is not considered a large scale.
(3) The usage of ChatGPT is a new technology which needs additional care and understanding of how potentially sensitive personal information is processed. For example, if chat data is used by Open AI to train ChatGPT.
(4) The target community are individuals with disabilities like hearing or speech impairments which is considered a vulnerable population.

Cookie Usage Analysis

An analysis was performed using Cookiebot (www.cookiebot.com) to determine what cookies are used and for which purpose (full cookiebot report shared separately).

Information Security Analysis

Several areas were reviewed to determine what threats that may occur and how to avoid data breaches which have large penalties in light of GDPR. Data breaches can occur not due to technical problems but simply using social engineering and stealing login credentials if not properly handled or losing a company computer.

Login Credentials

Credentials are not shared within the team. Not everybody has MFA implemented to prevent login credentials from being stolen and to prevent unauthorised login. Recommend consistent activation of MFA by team.

AP1: MFA needs to be implemented by whole team

When connecting with SSH custom certificates are used unique to each developer or devops.

Service Level Agreement

The SLA with both the ministry of interior and control centres with DEC112 association stipulates that all data shall be transferred or destroyed. Important to stipulate exact conditions such information is transferred or destroyed. The destruction of the data shall be documented. The potential transfer of DEC112 service to another entity also needs to be stipulated. For example transfer can be limited to registration information

AP2: Update of DEC112 association policy for covering 3 data handling scenarios: a) what data can be transferred, b) how to handle transfer of DEC112 operations to another entity and c) if DEC112 terminates SLA with ministry of interior steps for destructing collected information.

Funded by the European Union

The SLA is missing a third party list and what are the privacy rights of an individual. The SLA is not clear what data can be transferred and needs clarification. The role of DEC112 being only a data processor or a data controller also needs to be clear. If for example, DEC112 through the app is a data controller for registration and communication it sets a clearer separation than what other data controllers may request for.

AP3: Update ministry of interior and control centre SLA with the latest list of third parties and clarify what data may be accessed.

Security Clearance

Providing emergency services deals with highly sensitive communication. The ministry of interior requires that all those with access to DEC112 are not in the police registry. The requirement is documented in the SLA.

AP4: Check everybody with access to DEC112 has copy of police registry

Violations

There is strong language in the SLA by the ministry of interior when there is misconduct and if it is proven that somebody intentionally jeopardised the DEC112 service they will be prosecuted. Important to have clear DEC112 association policy violations may be prosecuted.

Privacy Policy

The privacy policy should convey in a clear language for deaf people to understand how their personal data is used. A review of the privacy policy showed that it is incomplete and needs updating. These are a sample of some websites with the structure and composition that is recommended for DEC112.

https://telldus.com/telldus-privacy-policy/

https://portal.life-guard.dk/website/privacypolicy

AP6: Update privacy policy with new template ensuring it is understood by target

When the privacy policy is updated a cookie analysis should be performed using Cookiebot (www.cookiebot.com) to determine what cookies are used and for which purpose. The following webpages will be analysed for cookie usage

https://www.dec112.at/en/web-privacy/

https://www.dec112.at/privacy/

https://www.dec112.at/privacy-idaustria/

Review of systems

This section is a review of the systems used by the DEC112 association. A complete inventory of the systems can be found in the "Third-party list" report. These systems were found to potentially handle personal information at a larger scale.

The following third-party systems are in the process of being phased out specially in considerations of the data transfer issues to non-EU countries.

- Matomo (https://matomo.org/)

Actions Summary

This is a summary of the actions and priority.

AP	Priority/Status	Title	Description
AP1	M / open	Consistent usage of MFA (ticket #81)	MFA needs to be implemented by whole team
AP2	M / open	DEC112 association policy on data handling (ticket #38, #93)	Update of DEC112 association policy for covering 3 data handling scenarios: a) what data can be transferred, b) how to handle transfer of DEC112 operations to another entity and c) if DEC112 terminates SLA with ministry of interior steps for destructing collected information.
AP3	M / open	Ministry of interior SLA update (ticket #84)	Update ministry of interior and control centre SLA with the latest list of third parties and clarify what data may be accessed.
AP4	L / finished	Police registry (ticket #94)	Check everybody with access to DEC112 has copy of police registry
AP5	L / finished	Policy on violations	Add policy to increase awareness of consequence of violations by any member
AP6	M / open	Privacy policy update (ticket #86)	Update privacy policy with new template ensuring it is understood by target group

AP7	L / finished	Replace analytics and debugging tools (ticket #36)	Replacement of Google Firebase Crashlytics, Sentry and Google Analytics

Table A.1: Actions and Priorities

Further Information: Understanding GDPR

Fundamental Rights

Like freedom of expression and religion every EU citizen has a fundamental right for protection of personal data. Here is the text in Article 8 which is the basis for GDPR.

Article 8

Protection of personal data

1. Everyone has the **right to the protection of personal data** concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Objectives

Each employee is responsible to raise questions relating to how an organisation manages internal routines that may have a GDPR impact. If the employee has a better understanding of GDPR and applies the knowledge on day to day activities, even in their private activities, they are better able to catch GDPR violations. The consequences of some of the data breaches occurring daily are huge financial impacts and in some cases threat to their own life. A good personal motivator to be interested is to ask the question if you trust how your personal data is being handled.

The objective of this section is to help each employee understand what to look for if any routines should be changed or check if any new services or systems are introduced. To help get a basic grasp of GDPR the following topics are covered:

1. What is considered personal data?
2. What principals should be followed to process personal data?
3. When is consent required?
4. What are the personal rights that need to be prepared to be answered?

What is considered personal data?

If no personal data is exchanged or if personal data is anonymized, then there is no GDPR concern and no risk of data breach risks.

What to look for when personal data is collected. Three types of personal data: identifiable, quasi-identifiable and sensitive. The quasi-identifiable example: even if no identifiable information is shared, if enough attributes like gender, data of birth and zip code are available it is possible with high accuracy to re-identify an individual. If sensitive information is collected with identifiable and quasi-identifiable attributes, then additional precautions are required and possibly a risk assessment like a DPIA is necessary.

Identifiable	Quasi-identifiable	Sensitive
name ID (example driver's licence #) physical address e-mail photo IP address * GPS location **	(combination of attributes) gender, date of birth, and postcode	ethnic background political views religion physiological (DNA) mental (medical diagnosis)

Note:
* an IP address can be tied to an individual and home. Note: As a private citizen you protect yourself from this insight by using a VPN service. You also need to use private mode so cookies are not used as fingerprints which can re-identify you.
** GPS location can track where you visit and where you live and is considered personal data

There are more examples but this is a basic introduction of what is considered personal data.

What principals should be followed to process personal data?

All organisations that process personal data need to abide by the principles set by GDPR chapter 2. The principles help understand what to focus on when evaluating the practices of a system or routine. For example, how a privacy policy is written should reflect these principals.

- **Lawfulness, fairness and transparency:** Processes shall be done lawfully, fairly and in a manner that is transparent for the intended use.
- **Purpose limitation:** Processing of personal data shall have a legitimate purpose and limited to needs to fulfil the purpose. Additional data cannot be incompatible with the scope. For example, a cooking app shall not be collecting location information.
- **Data minimization:** To avoid collecting too much information the processing of personal data shall be minimised.
- **Data accuracy:** The collected personal data shall be accurate and be kept up to date.

- **Storage limitation:** The collected data shall be limited for the duration that is necessary.
- **Integrity and confidentiality:** Processes shall be done in a manner that ensures appropriate security of the data.
- **Accountable:** It shall be possible to demonstrate compliance to these principles.

When is consent required?

A legitimate purpose for processing personal data does not require a consent but if additional services are offered that go beyond the original purpose then a consent is required. For example, a web page may provide a news service but to store a cookie to track that pages you view and offer targeted ads requires a consent. The consent must be opt-in meaning choice cannot have a default of on. Unfortunately, frequently the option to opt-out is hidden. A good example is following notice with clear consent.

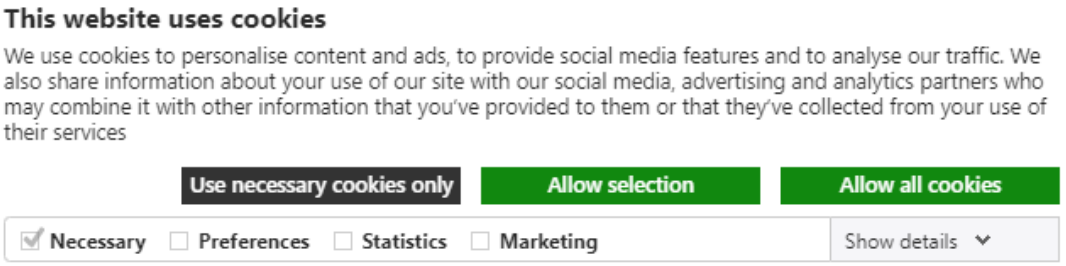

Figure A.1: Example of Well-Implemented Website Cookies Consent Interface

When checking out a service, it should not be misleading or hide how to consent. Below is an example of a misleading consent. **TIP:** Instead of typically clicking “agree” choose to “Manage settings” and scroll to the bottom. Typically most options are default off but you need to scroll to the bottom to “Save and continue” with them off. The marketing companies are making it just a little harder so 80% of the visitors simply select “I agree”. I call this death by consent so you do not care how personal data is collected for marketing purposes.

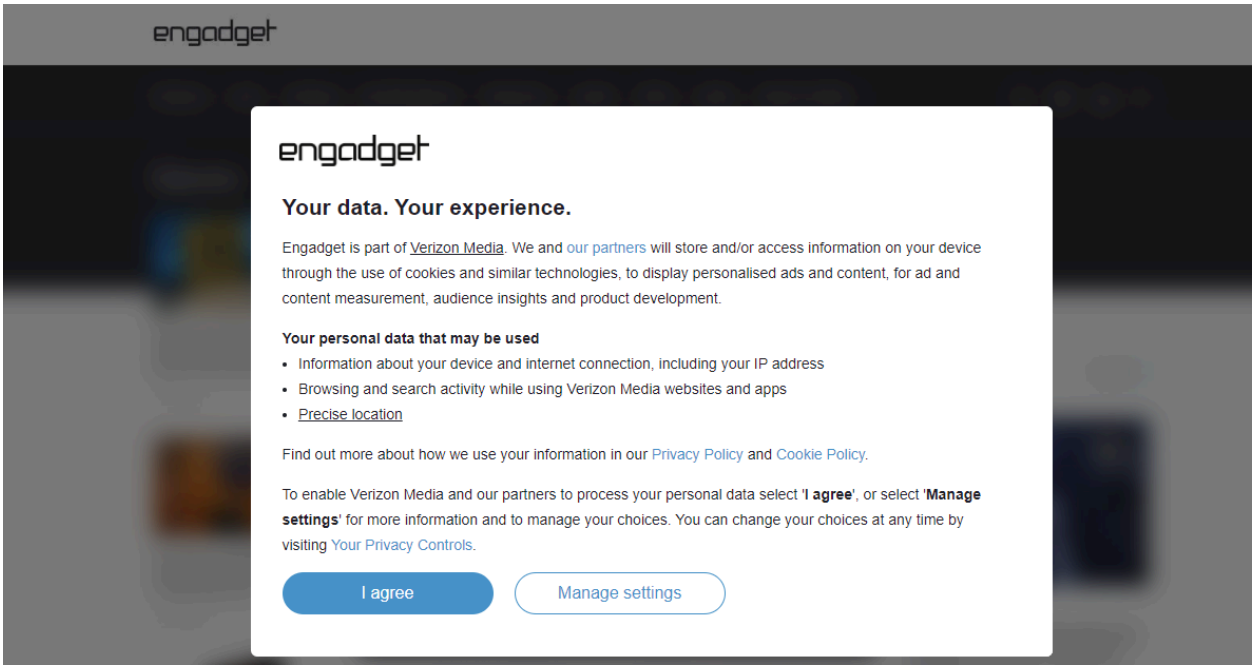

Figure A.2: Example of Poorly Designed Website Consent Interface

What are the personal rights that need to be prepared to be answered?

The final area to understand are the personal rights of an individual. The rights can be found in GDPR chapter 3 but before going into the rights good to be aware of some terms relating the roles surrounding data processing.

The individual is a Data Subject in GDPR terms. An organisation who has main responsibility for the Data Subjects personal data is called Data Controller. The Data Controller will not always or quite frequently rely on another company to collect the data on their behalf. The other company is a Data Processor. An organisation, Data Controller, needs to review the Data Processor routines and make sure the same processing principles and Data Subject rights are met.

The following table lists the rights of an individual, Data Subject, which an organisation, Data Controller, needs to be prepared to answer.

Rights	Description
The right to be informed	The individual has a right to be informed of any matters relating to processing of the personal data that may affect them. For example, in case of data breaches or changes to the privacy policy.
The right of access	The individual has a right to view their personal data.
The right to rectification	If the personal data is incorrect, they have the right to have it corrected.
The right to erasure	In the case they do not want the personal data to be kept they can request that the personal data is erased.*
The right to restrict processing	If the individual requires special consideration when processing the personal data to avoid exposure to any risks, they can request to restrict the access to the data.
The right to data portability	The individual has the right to not only access their personal right but right to move their data to another service provider. This is easier said than done due to compatibility issues.
The right to object	If any of their rights are impacted, they have a right to object
Rights in relation to automated decision making and profiling.	In case of automated decision making or profiling based on personal data which has direct impact they have the right to request to perform manual decision making.

Table A.2: GDPR Rights

* Not all personal data can be erased and there may be other legal requirements in a country where data must be kept for a longer period. For example, salary information must be kept for 7 years in Austria. Even though personal data is kept for a longer period it is only for the purpose of fulfilling the legal requirement and the data cannot be used for any other purpose.

LINALTEC

DEC112 DPIA Report

Assessment

Date: 2024-03-29

LINALTEC AB
Assessment by:
Jan Lindquist (GDPR Privacy Advisor)
jan@linaltec.com
+46 730 694 942

Funded by the European Union

History

2023-08-31 - initial Version

2023-10-20 - first update: minor changes in text to improve clarity, add references in Table B.10 to DEC112 JIRA ticketing system and current status of actions

2024-01-19 - second update: feedback from Ruben Roex (Timelex) incorporated. Clarified retention justification and security and privacy implementation responsible.

2024-03-29 - final version: AP9 closed and SIP information can be removed from Kamailio database. AP11 was closed, chatgpt usage policy was specified in D2 delivery. AP12 right to be forgotten has been completed. AP15 and security risk #3 is addressed by limiting 1 sms per minute, resend limited to 5 requests.

Introduction

Purpose

DEC112 provides emergency service based on text messages targeted for individuals with disabilities like hearing or speech impairment. DEC112 commits to manage compliance with applicable personal data protection legislation, contractual requirements and other internal policies.

This report is a Data Protection Impacts Assessment with intention to describe the processing of personal data and minimising the risks as much as possible.

Glossary

Term	Description
Data Protection Agency (DPA)	The Data Protection Agency is responsible for enforcement of GDPR. They are the point of contact for data breaches or questions.
Data Protection Impact Assessment (DPIA)	A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible.
Data Protection Officer (DPO)	The Data Privacy Officer is appointed at DEC112 to manage all privacy questions and ensure the organisation is fulfilling training and security measures.
GDPR	The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

Term	Description
Individual	The term individual refers to the end-user who uses the coaching service.
Organisation	The term organisation refers to the whole DEC112 association members and subcontractors
Personal Identifiable Information (PII)	The term PII is used to refer to any personal identifiable information like email, name or driver's licence. Some PII data can be directly linked to an individual and some can be extrapolated like GPS location or physical characteristics.

Table B.1: DPIA Glossary

Scope

The resources that are in the scope of the DEC112 DPIA are:

- Software
  - DEC112 platform and application
  - 3rd party software suppliers
- Partners
  - Data processing agreements with DEC112 platform

Roles and Responsibilities

These are the roles at DEC112 and the responsibilities to provide accountability.

Role	Responsibility
Everybody	It is the responsibility of every employee and contractor to be observant of the privacy related irregularities and report them to the DPO immediately. The incident will be logged to best determine action.
Leadership team	Commit to the privacy policy and ensure the privacy program led by the DPO is being fulfilled.
IT admin	Ensure all access to private data is restricted based on role.
Platform Development	During the development phase limit the usage of real personal data.
Research	Research shall be performed on anonymized data but due to the level of detail of re-identify additional security measures shall be followed.
Data Protection Officer	Manage the privacy program and ensure adequate controls and training are in place minimising all privacy risks.

	Provide regular updates to the leadership of the privacy KPI's. The role is assigned to the vice-president of DEC112.
Chief Technical Officer	The implementation of security requirements and ensuring the solution follows privacy-by-design is the responsibility of the president of DEC112.

Table B.2: Roles and Responsibilities

Scope of Processing

Processing Overview

The following diagram represents the processing of the DEC112 solution. The main components are the DEC112 app and the DEC112 Core-Services. The Reg-API's components are gateways to the external services for the purpose of user verification. There are test simulation components to help to get individuals used to the app and interaction with operators during an emergency.

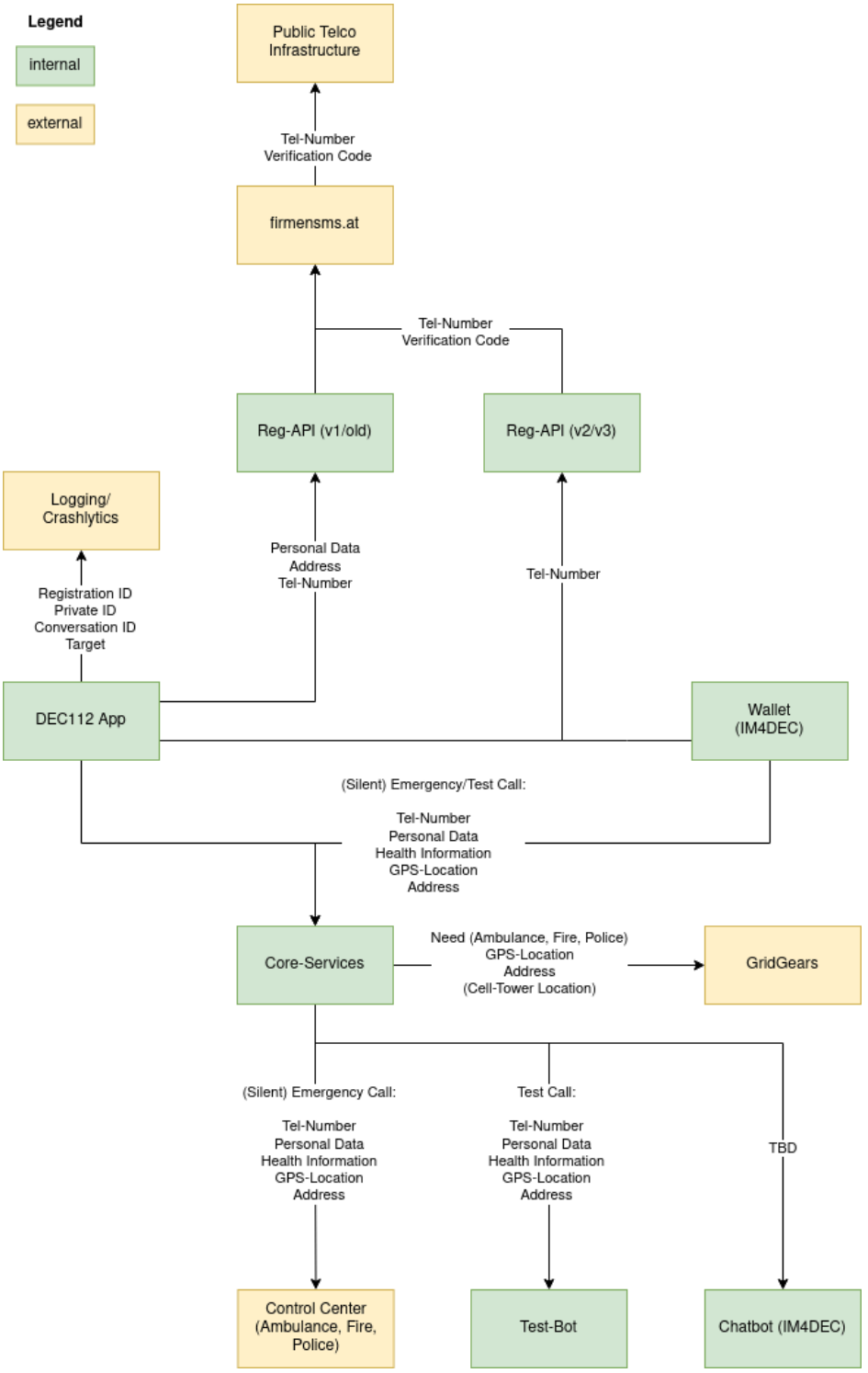

Figure B.1: Processing Overview

AP8: The DEC112 App is meant to be a 3rd party provider and a DPA should be in place.

These are the main flows when processing personal data:

1. Registering first time using the app
2. Emergency simulation with test bot or in the future chat-gpt
3. Emergency call

Data Subjects

The data processing is limited to individuals in Austria.

- Data will be collected when first registering with the DEC112 app.
- Data subjects may share additional information from Apple Health or Google Health during the registration.

Data Types

There are various different types of data to be processed by the system. The table below lists the data types and provides a definition for each.

Data Type	Definition	Example
Personal Data	The personal data has the following information: identifying, physical characteristics, demographics and medical health.	name, height, weight age, gender, disability (ex. hearing, speach), diagnosis, medical conditions, free text
Tracking	The tracking information comes in different forms: contact, location and computer device.	email, physical home address, mobile number, GPS coordinates, IP address, model, device id
Communication	The communication is limited to text, no voice. These occur during an emergency or simulation of an emergency.	Text messages

Table B.3: Data Types

Personal Data Classes

This section describes how personal data will be collected, used, transferred and if necessary, kept up to date. The privacy class are broken down into following classes:

- **PII**: Personal Identifiable Information

Specific information that references an individual, such as name or an identification number.

- **QII**: Quasi-Identifiable Information

Any piece of information (e.g. a geographical position in a certain moment or an opinion about a certain topic) that could be used, either individually or in combination with other quasi-identifiers, by someone that has knowledge about that individual with the purpose of re-identifying an individual in the dataset

- **SEN**: Sensitivity

The following type of information is considered sensitive: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Categories

The following table lists the data collected (right column) and Data Type Name, Personal Data Category and Privacy Class. Special attention is required for privacy class of type SEN (sensitive). Everybody in the organisation shall be able to identify processed personal specially sensitive information like disabilities. When they come across they should be extra cautious with the processing of the data. If unintentionally exposed, consider it a security incident and report it for remediation. recognize when they come across sensitive data that are not classified in the table.

Data Type Name	Personal Data Category (1)	Privacy Class	Data collected
Personal Data	Identifying	PII	name
	Physical characteristics	QII	height, weight
	Demographics	QII	age, gender
	Medical health	QII/SEN	disability (ex. hearing, speach), diagnosis, medical conditions, free text

Data Type Name	Personal Data Category (1)	Privacy Class	Data collected
Tracking	Contact	PII	email, physical home address, mobile number
	Location	QII	GPS coordinates
	Computer device	QII	IP address, model, device id
Communication	Text communication	SEN	Text communication

Table B.4: Data Categories

Note: (1) DPV related material for setting category. First link is a nice overview diagram. The second and third links are standards work in the W3C Data Privacy Vocabulary (DPV) community group.
https://enterprivacy.com/wp-content/uploads/2018/09/Categories-of-Personal-Information.pdf
https://dpvcg.github.io/dpv/#vocab-personal-data-categories
https://w3c.github.io/cg-reports/dpvcg/CG-FINAL-dpv-pd-20221205/

Data Retention

The data retention shall be strictly adhered to. The justification for retaining for the specified period is explained.

Data Type	Retention	Retention Justification	Retention Measure
Personal Data	All personal data is stored in the DEC112 app and is not deleted if an individual does not delete the app installed on their phone.	Individuals have full control of the app and are able to delete it at any time. From app individual can have all SIP user in Kamailio database information removed.	
Tracking (Contact, Computer device)	During registration some tracking information like phone number and model are stored in the DEC112 backend. The information is stored for 24 hours. .	The registration information is only kept for a limited time in the system .	

Data Type	Retention	Retention Justification	Retention Measure
Communication	All emergency communications - once routing is established - are forwarded to the operator together with personal data and tracking information. The DEC112 backend stores the communication log for 2 years.	The communication is retained as long as necessary to provide evidence of delivering emergency service as part of contract with the Ministry of Interior. An example, the data is used to check potential abuses by callers when a call is not a real emergency.	

Table B.5: Data Retention

AP9: The backup of the app data has to consider the retention period and how to forget if there is a request.

Data Access/Use

Access to the data at DEC112 is broken down into the following roles.

Data Type	IT Admin	Research
Personal Data	yes	yes (1)
Tracking	yes	yes (1)
Communication	yes	yes (2)

Table B.6: Data Access/Use

Note (1) - Personal data has to be generalised to demographics so no re-identification is possible. For example, change birthdays to an age range like 40-50. Another example is statistics based on location, the aggregate number of individuals for a given region cannot represent less than 10 individuals. If the number of individuals in a region is lower than 10 then that region needs to be combined with another region to represent more than 10 individuals.

Note (2) - Text may be used for research and understanding performance of chat bots like chatgpt.

AP10: Reports created based on personal data and tracking requires a policy describing the generalisation of the information.

Data Sharing

The instances that data may be shared from DEC112 are the following:

1. Routing information is shared with the Ministry of Interior for the purpose of controlling which emergency service was used. One reason for sharing information is to identify and track fraudulent requests for emergency services and charge for falls dispatch. All emergency communications to the police require the police to respond.
2. The emergency communication is forwarded to the control centre on an instance basis. Once a session is terminated the DEC112 app does not keep a copy of the instance. The control centre retains information for 90 days but is dependent on their own policies.

Compliance with Data Protection Law

The following sets out the lawful bases for the processing of personal data identified.

Lawful Basis for Processing of Personal Data in Emergency Calls

The following lawful basis in Article 6 and Article 9 of the GDPR are appropriate to and suitable for the purposes of processing personal data for providing emergency services.

Article 6 (Lawfulness of processing)

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6.1(e); (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller).

Article 9 (Processing of special categories of personal data)

Processing is necessary for the purposes of providing emergency care during an emergency and medical diagnosis and treatment of the individual or other emergency if that is fire or police related.

Exercise of Data Subject Rights

An individual has the following rights and what are the actions taken.

Privacy Right	Description	Response	Internal routine
Right of access	Individuals have the right to access all collected personal data.	DEC112 app provides access to all collected information.	
Right of rectification	Individuals have the right to have any collected information rectified.	DEC112 app allows individuals to make any correction.	
Right to be forgotten	Individual has the right to be forgotten	Through the DEC112 app individuals have the ability to remove or have all their data forgotten. To remove backend registration information, it needs to be communicated for a manual removal.	IT department
Right to restriction of processing	Under special circumstances the individual may request that personal data is not processed or removed. This may occur under circumstances when an individual wants to raise concerns with DPA.	Questions of restricting access shall be directed to the IT department and DPO shall be involved in order to determine nature of the request and establish reasonable reason for request.	IT department

Privacy Right	Description	Response	Internal routine
Right of portability	Individuals have the right to request to port personal data to another service.	DEC112 app is not an open platform for data portability. Data sources like Apple Health provided the portability if requested.	
Right to object	Individuals have the right to object to processing of personal data and shall inform the organisation of the objection.	DPO shall be involved in order to determine the nature of the request and establish reasonable reason for request.	

Table B.7: Exercise of Data Subject Rights

International Transfers

No personal data is transferred out of the EU except for application crash diagnostics used in Google Firebase Crashlytics.

Appointment of Data Processors

All of the data processors are appointed under Data Processors Agreements in compliance with Article 28 of the GDPR.

Identify and Assess Risks

The table below sets out the risks that have been identified for the project and the levels for those risks if not mitigated. Overall risk score for each risk identified is calculated as the product of the risk likelihood score and the risk impact score (i.e. likelihood score X impact score). The following sets out the metrics used in documenting the risk assessment.

Likelihood	Score
Highly Unlikely	1
Unlikely	2
Possible	3
Likely	4
Highly Likely	5

Impact	Score
Negligible	1
Minor	2
Moderate	3
Major	4
Critical	5

Overall	Score
Low	1-7
Medium	8-14
High	15-25

No.	Risk	Likelihood	Impact	Likelihood Score	Impact Score	Overall Risk
1	Sharing of logs: Sharing of logs which may have personal information may be shared using Google Drive or Slack. Logs with potential emergency communication should be limited and deleted once addressed.	The likelihood is very limited with only 20% of communication being an emergency so sensitivity may be limited.	If sensitive communication is accessed it will be considered a security breach and needs reporting.	2	4	8
2	Chatgpt biases during simulated chat: The chatgpt may have biassed communication which may confuse or mislead an individual.	The responses will likely not be perfect.	These are only simulated chats and will be clearly communicated with individuals.	3	2	6
3	Fixed registration API keys: The registration API uses a fixed key used during registration of new users. After registration is performed a unique key is stored specifically for the device.	A man in the middle attack may be used to access the key.	Fake registration may cause sms spam which may affect reputation and high sms costs.	4	5	20

No.	Risk	Likelihood	Impact	Likelihood Score	Impact Score	Overall Risk
4	Consistent usage of MFA: Production environment access should be only supported using MFA. Development environment may also need MFA in order to prevent injection of malicious code.	If a computer is hacked, stealing credentials is easy.	Depending on the level of privileges the whole system may be interrupted, corrupted or worse ransomware is installed.	3	5	15

Table B.8: Risk Assessment

Identify Measures to Reduce Risks

An evaluation of the identified risks in the previous section has been carried out and a series of measures have been detailed that seek to mitigate those risks to an acceptable level. The table below sets out these mitigation measures and an assessment of the risk impact due to their introduction.

No.	Risk	Mitigation	Likelihood Score	Impact Score	Overall Risk	Remaining risk to data subject
1	Sharing of logs	Reduction: Limit of sharing of logs to a single system and awareness to limit sharing sensitive communication. (AP13)	2	4	8	Data breach space is reduced
2	ChatGPT biases during simulated chat	Reduction: Close evaluation during prototyping and feedback from users (AP14)	3	2	6	Improved perception of users of chatbot.
4	Consistent usage of MFA	Reduction: require MFA and also increase security awareness	3	5	15	Data breach is reduced by additional step in

No.	Risk	Mitigation	Likelihood Score	Impact Score	Overall Risk	Remaining risk to data subject
		[AP1]				logging into system

Table B.9: Measures to Reduce Risks

Actions Summary

This is a summary of the actions and priority.

AP	Priority/ Status	Title	Description
AP8	H / open	DEC112 App DPA (ticket #36)	The DEC112 App is meant to be a 3rd party provider and a DPA should be in place.
AP9	M / finished	DEC112 App backup (ticket #36)	The backup of the app data has to consider the retention period and how to forget if there is a request.
AP10	M / open	Policy for exporting usage reports (ticket #31)	Reports created based on personal data and tracking requires a policy describing the generalisation of the information.
AP11	M / finished	Policy for usage of communication for creating chatbot (development in the course of IM4DEC project)	Usage of text communication for building chatbot like ChatGPT has to be strictly controlled and anonymized. No names or addresses shall be included, nor personal data or tracking details. They shall be kept separate.
AP12	L / finished	Policy for applying right to be forgotten (ticket #86)	The routines for right to be forgotten in the backend should documented
AP13	M / open	Sharing of logs (ticket #82)	Risk #1
AP14	L / in progress	ChatGPT biases during simulated chat (see ChatGPT Privacy Assessment - Appendix C)	Risk #2
AP15	H / finished	Fixed registration API keys (new RegAPI in the course	Risk #3

AP	Priority/ Status	Title	Description
		of the IM4DEC project)	

Table B.10: DPIA Action Summary

Appendix C - ChatGPT Privacy Analysis

History

2023-08-31 - initial Version

2023-10-20 - first update: minor changes in text to improve clarity, sent to Ruben Roex from Timelex for review, add reference to implementation for Table C.1

2024-01-19 - second update: feedback from Ruben Roex (Timelex) incorporated. The new Terms of Use being released on February 15, 2024 introduces a data controller dedicated to the European Economic Area (EEA). The new “sharing publication policy” clarifies how the ChatGPT generated content shall be communicated externally.

2024-03-29 - final version: updated system prompt in Table C.1 based on user feedback

Overview

The association DEC112 plans to use ChatGPT, Large Language Models (LLMs) from OpenAI in order to improve the user experience. DEC112 is an emergency service for deaf people and recently expanded to support silent emergency notifications. Intention is to use ChatGPT for simulation purposes only for an emergency chat. Emergency chats are considered highly sensitive. ChatGPT will ONLY be used for simulation purposes and simulates responses from an operator. Clear indication that it is a simulation will be provided and the user will have the opportunity to rate conversations and consent to sharing chat data.

What is the DEC112 role in relation to OpenAI? OpenAI processes “customer data” and is defined as a Data Processor. Organisations using OpenAI services are Data Controllers and therefore need to be aware of the repercussions of using ChatGPT.

Executive Summary

These are the main findings so far of using ChatGPT in the IM4DEC project.

- ChatGPT API has a default of not using user data for training ChatGPT BUT the browser based ChatGPT is the contrary which is a major concern. Browser-ChatGPT requires users to opt out otherwise user data is used to train ChatGPT. A form has to be filled to

explicitly make the request and it is necessary to indicate that it is not only browser but device since they are not synced.
- Preparing ChatGPT for simulating emergency conversations can be done in one of two methods which is described below.
- Additional procedures are required for how to handle conversations through a new policy so all those administering the DEC112 app and access to simulated or real conversation are aware of the risks and precautions to be taken.
- Regulator routines need to be established to ensure the answers from ChatGPT are trustworthy and ethical. Incorrect answers or abuse of the simulated conversation may expose DEC112 to bad press and litigation.

European Terms of Use: https://openai.com/policies/eu-terms-of-use

Analysis

OpenAI Policy Analysis

There are key questions relating to using ChatGPT which need answering in order to understand the consequences:

1. Are ChatGPT conversions kept confidential?
2. Are conversation histories used to train ChatGPT?
3. Any security considerations when using ChatGPT?

The policies are continuously being updated so analysis is a snapshot from July 26th, 2023. Quotes from the policies are included to better explain the conclusions in this analysis. There are also links to the original policy.

Open AI Privacy policy: https://openai.com/policies/privacy-policy

Claim 1: Input data is used for training the chatgpt model, opt-out is required

“As noted above, we may use Content you provide us to improve our Services, for example to train the models that power ChatGPT. See for instructions on how you can opt out of our use of your Content to train our models.”

Open AI - Data Controls FAQ: https://help.openai.com/en/articles/7730893-data-controls-faq

Claim 2: When opted-out input (conversation) is not used to train chatgpt
“Data controls offer you the ability to turn off chat history and easily choose whether your conversations will be used to train our models.”

“While history is disabled, new conversations won’t be used to train and improve our models,

Claim 3: Ensure no browser add-ons or malware on computer stores conversation
“Please note, this will not prevent unauthorised browser add-ons or malware on your computer from storing your history.”

Claim 4: Opting-out is on a device/browser basis. Need to opt-out independently.
“This setting does not sync across browsers or devices.”

same as Claim 1
“Our large language models are trained on a broad corpus of text that includes publicly available content, licensed content, and content generated by human reviewers. We don’t use data for selling our services, advertising, or building profiles of people—we use data to make our models more helpful for people. **ChatGPT, for instance, improves by further training on the conversations people have with it, unless you choose to disable training.**

Claim 5: History can also be disabled and will be removed after 30 days.
While history is disabled, new chats will be deleted from our systems within 30 days”

Claim 6: There are plans by OpenAI to simplify opting-out
“We are working on a new offering called ChatGPT Business that will opt end-users out of model training by default. In the meantime, you can opt out from our use of your data to improve our services by filling out this form. Once you submit the form, new conversations will not be used to train our models.”

Open AI - API data usage policies: https://openai.com/policies/api-data-usage-policies

Claim 7: Using the API by default the submitted data is not part of the training and requires opt-in
As of March 1, 2023

1. OpenAI **will not use data submitted by customers via our API to train** or improve our models, unless you explicitly decide to share your data with us for this purpose. You can
2. Any data sent through the API will be retained for abuse and misuse monitoring purposes for a maximum of 30 days, after which it will be deleted (unless otherwise required by law).

Claim 8: File endpoint is retained until user deletes the file
“Data submitted by the user through the Files endpoint, for instance to fine-tune a model, is retained until the user deletes the file.”

How your data is used to improve model performance: https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance

Claim 2: same as claim 2
"...to turn off training for any conversations created while training is disabled or you can submit this form. Once you opt out, new conversations will not be used to train our models."

Data Processing Agreement
The data processing agreement (DPA) needs to be requested separately and is not provided directly so no link provided.

Claim 9: Requests from law enforcement or public authority will inform customer
"Customer. OpenAI will inform Customer if OpenAI becomes aware of:

a. any legally binding request for disclosure of Customer Data by a law enforcement authority, unless OpenAI is otherwise forbidden by law to inform Customer"
b. any notice, inquiry or investigation by an independent public authority established by a member state pursuant to Article 51 of the GDPR (a "Supervisory Authority") with respect to Customer Data"

Sharing Publication Policy: https://openai.com/policies/sharing-publication-policy
When using ChatGPT service and sharing the output it is important to abide by these practices:

a. The generated content should be attributed to organisation (DEC112) and clearly indicate content was AI-generated. Note - The badge to be used to indicate it is OpenAI generated can be found in the Brand guidelines.
b. The content should not violate the Content Policy which in essence shall not harm yourself or others

Summary

Here is a summary of the main points from OpenAI policies for consideration.

Claim 1: Input data is used for training the chatgpt model, opt-out is required.
Claim 2: When opted-out input (conversation) is not used to train ChatGPT.
Claim 3: Ensure no browser add-ons or malware on computer stores conversation.
Claim 4: Opting-out is on a device/browser basis. Need to opt-out independently.
Claim 5: History can also be disabled and will be removed after 30 days.
Claim 6: There are plans by OpenAI to simplify opting-out.
Claim 7: Using the API by default the submitted data is not part of the training and requires opt-in.
Claim 8: File endpoint is retained until the user deletes the file.
Claim 9: Requests from law enforcement or public authority will inform customers.

Guidelines for Using Generative AI Tools

The Canadian Cyber Security Guidance[6] provides a good set of guidelines. Much of the guidance is focused on the security aspects and mitigation. What concerns this analysis is how the AI tool is used. The following text comes from the guidance.

> **Security protections when using generative AI tools**
>
> The following security measures can help you generate quality and trusted content while mitigating privacy concerns:
>
> **Establish generative AI usage policies** — The policies should include the types of content that can be generated and how to use the technology to avoid compromises to your sensitive data. Your policies should also include the oversight and review processes required to ensure the technology is used appropriately. When creating solutions using generative AI, ensure practices lead to trustworthy and ethical behaviour. Be sure to implement the policies quickly and ensure they are communicated to staff.
> **Select training datasets carefully** — Obtain datasets from a trusted source and implement a robust process for validating and verifying the datasets, whether they're externally acquired or developed internally. Use diverse and representative data to avoid inaccurate and biassed content. Establish a process for outputs to be reviewed by a diverse team from across your organisation to look for inherent biases within the system. Continuously fine-tune or retrain the AI system with appropriate external feedback to improve quality of outputs.
> **Choose tools from security-focused vendors** — Ensure your vendors have robust security practices baked into their data collection, storage, and transfer processes.
>
> **Be careful what information you provide** — Avoid providing PII or sensitive corporate data as part of the queries or prompts. Determine whether the tool allows your users to delete their search prompt history.

Conclusion is that there has to be policies in place for the usage of the AI tools, a clear understanding of the training dataset and if search history can be deleted.

[6] https://www.cyber.gc.ca/en/guidance/generative-artificial-intelligence-ai-itsap00041

Using Own Data Analysis with ChatGPT

Model 1: Create snapshot of conversation and reuse in new conversations

With ChatGPT it is possible to create a backup of the communication with ChatGPT that can serve as a starting point for new communications. This allows starting new conversations from that backup and keeping them independent.

Model 2: Use own instance as plugin to ChatGPT

This approach requires more effort but gives more control over your own data. It is possible to add own data to ChatGPT without divulging any data through a plugin. There are many plugins already developed for ChatGPT that allow enhancing the functionality. ChatGPT uses a corpus for training that extends to September 2021. The method with plugins allows you to add your own data.
Here is an example of a Medium article on how to create a private ChatGPT with your own data[7].

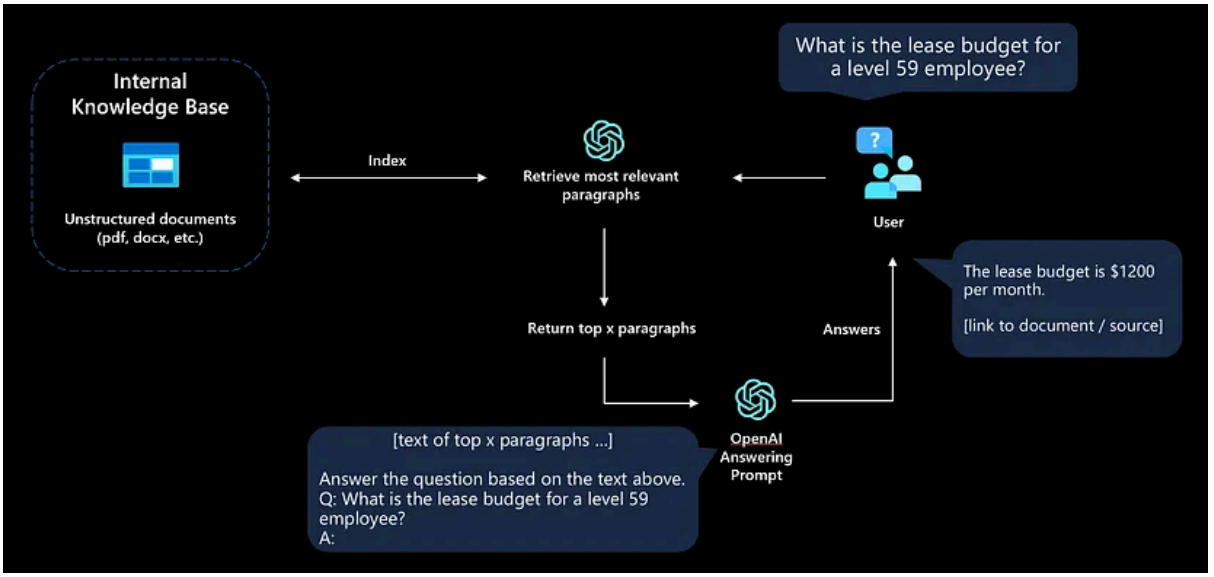

Figure C.1: ChatGPT Plugin

[7] https://medium.com/@imicknl/how-to-create-a-private-chatgpt-with-your-own-data-15754e6378a1

Prompt Based Fine Tuning

System Instructions

The ChatGPT “system” role needs to get clear instructions on how to converse. The following table has the requirements and text to instruct the system role in the IM4DEC project.

Reference to current implementation on Github: https://github.com/OwnYourData/dc-chatbot/blob/main/config/textblocks/OAI_system_default_en.txt

Requirement	Instructions
Set control operator role	You are an emergency services assistant who is a control operator routing emergency calls dedicated to hearing and speech impaired.
Short concise responses	The conversation has to be concise since the caller is hearing and speech impaired and is used to short precise conversations. It is very important to ask only one question at a time.
Do not sound apologetic	Do not sound apologetic in conversation and do not say “I am sorry” or “Thank you for providing the information”.
Handling initial response and consider available location information	The initial response might include address and the type of emergency. Try to parse this information and consider it in the subsequent communication. Be also aware that GPS data is automatically provided as the caller location.
Avoid repetition	Do not repeat questions about the emergency location or the address of the caller. Do not repeat information that emergency personnel are sent. Do not repeat questions about building access for emergency personnel.
Set order to check	Determine the following before sending emergency personnel:
Determine severity and nature of emergency	1) how serious is the problem and type of emergency, fire, medical, or police;

Requirement	Instructions
Determine where to send emergency	2) confirm that the provided GPS coordinates should be used to send emergency personnel to, or if another address should be used;
Determine if emergency has access	3) once emergency personnel is dispatched, only ask if personnel can get into the building if the type of emergency indicates it is in a building; and
Determine how caller will know emergency has arrived	4) only if the emergency is in a building ask if the caller can hear when emergency personnel arrive or are they hearing and speech impaired. In the case that emergency personnel cannot get into the building, inform emergency personnel what to do.
End call and indicate what kind of service will be dispatched	Once all information is gathered, end the call stating what type of emergency will be sent, ambulance, police or firemen. If the caller says “Stay on the line” do not end the call but otherwise end the call with the following text “I will end the chat, if something gets worse, restart the app immediately so I can help you further. The system has ended the emergency call. If you have any further questions, please call again.” If the call is not an emergency, end the conversation with “The system has ended the emergency call. If you have any further questions, please call again.”.

Table C.1: System Instructions