Proposal template Part B: technical description

PROFILA: A NEW-ERA DATA RELATIONSHIP PLATFORM

#@APP-FORM-HERIAIA@#

List of participants

Participant No. *	Participant organisation name	Country
1. (Coordinator)	De Roos Advocaten	Netherlands
2.	Universidad Carlos III de Madrid	Spain
3.	Partisia	Denmark
4.	Profila GmbH	Switzerland
5.	Publicis Bulgaria	Bulgaria
6.	Parhelium sp zoo	Poland

1. Excellence #@REL-EVA-RE@#

1.1 Objectives and ambition #@PRJ-OBJ-PO@#

Introduction

In today's rapidly evolving digital landscape, where algorithms govern our thoughts and actions, there is a pressing need for a solution that champions human intelligence, agency, privacy and meaningful digital relationships.

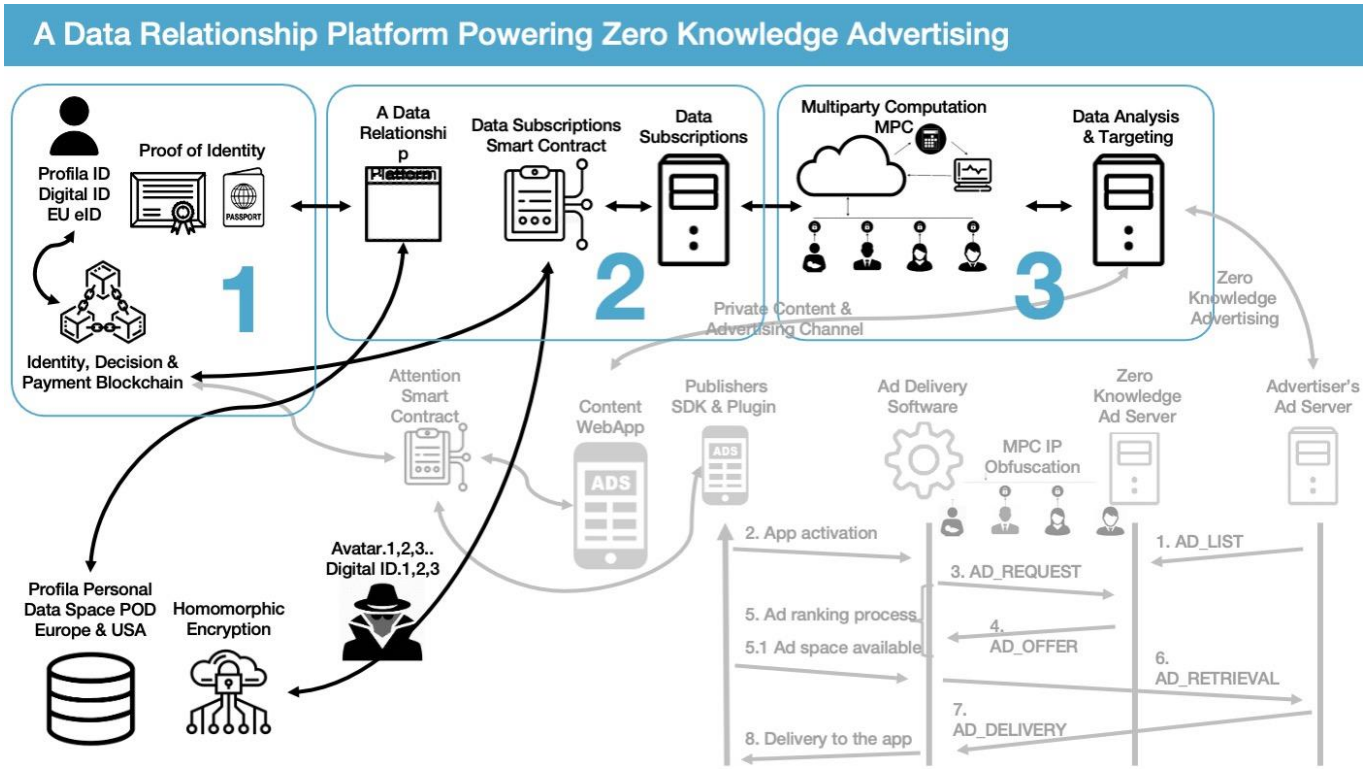
With this consortium, we want to build a platform that serves as a bridge between individuals and public companies or private entities ("brands"), fostering a mutually beneficial ecosystem where privacy, choice and value take centre stage. As we navigate the next era of AI-powered digital transformation, the consortium's goal is to ensure that humans retain sovereignty over their digital lives through smarter choices.

Our approach involves harnessing Web 3.0 and privacy-preserving technologies to empower individuals to create, own and share their most accurate and comprehensive personal data profiles. These data profiles encompass various facets of individuals' lives, including their preferences, sentiments and desires. Unlike traditional data profiles generated using first party data or observed behaviour, these new profiles are created and owned by the individuals themselves, guaranteeing authenticity, accuracy and longevity. By simplifying the process of sharing your profile with brands and people that individuals genuinely desire in their lives, we help to restore the balance of power in the digital landscape. Privacy is at the forefront of our platform, ensuring that individuals have full control over who accesses their data, fostering an environment of trust and transparency.

The benefits extend beyond individuals. Brands can leverage these accurate and detailed profiles to personalise their services, offering tailored content, special offers and information that genuinely resonates with their best customers, guests, patients, or employees. By tapping into the rich data provided and maintained by an individual, brands can deliver meaningful value and experiences throughout the customer's lifecycle, creating stronger connections with their most loyal audience.

The revenue model empowers individuals to license (but never sell) parts of their profile through data subscriptions while simultaneously managing their attention with brand content and advertising. This control is extended outside the platform's walled garden through our Zero Knowledge Advertising Protocol. This protocol, when implemented, will effectively replace the need for cookies on the internet and will implement active zero knowledge into mobile applications, browser and websites, making the internet personalised and private – the way it was meant to be.

The platform will be a people-controlled, Web 3.0 platform experience. By generating customer data, advertising and future e-commerce revenues from progressive brands, the platform will redirect revenues away from surveillance incumbents such as data aggregators or platforms such as Meta and Google. This helps to loosen the stranglehold these entities have on the market and contributes to solving the social dilemma by shifting audiences to a surveillance-free and algorithm-free environment, ushering into the European Union (EU) a much-needed competitive customer engagement and marketing platform. Through this comprehensive approach, we lay the foundation for a more equitable and empowering data driven digital EU economy.



State of the art – innovation

This application and the project it will manifest represents an extremely ambitious endeavour, not just in the cutting-edge technology it will develop and utilise, but in the creation of a new paradigm for data privacy, agency and sovereignty for all individuals. The results will be an aggregation of various technologies which are known but still lacking in real-world business models (blockchain, zero-knowledge proofs) and a business model which fully uses the potential of these technologies to create a better internet, an improved level of security and safety online and the empowerment of every individual.

The aggregation of these technologies will be combined with a new paradigm of empowered individuals who will find themselves with new tools and services to expand their agency and sovereignty online. They will create, manage and control the most accurate, authentic and valuable insights and information about themselves and have transparency as to who wants to communicate and interact with them and what they have access to. For the first time in the internet era, what is in an individual's head and what is in their heart, will be theirs to control and benefit from.

With such a radical departure to the current paradigm of surveillance marketing and social media control over personal data, our project will usher in a new era of possibilities which will bring new business models, innovation in products and services and ambitious initiatives built on top of our work.

Maturity Level

Profila has been researching digital privacy problems between 2019 – 2022, working together with the privacy department of CERN (European Organisation for Nuclear Research) and several prominent universities (Universidad Carlos III de Madrid on its zero-knowledge advertising research but also, for example, a privacy research project with University of Lucerne for Applied Sciences, sponsored by the Swiss innovation agency Innosuisse). Since beginning as a research initiative to understand the new paradigm of data privacy, individual-brand relationships and

how technology could solve some of the most pressing issues of the social media era, Profila has been involved in a thousand conversations with a range of stakeholders in order to understand the complete ecosystem and chart a path toward a better internet. Profila has met with privacy advocates, individuals of different backgrounds, brand marketers, data privacy lawyers, regulators, business owners, developers, investors, and a range of other stakeholders.

From this, a set of core values and a defined mission have emerged which are now finally being met with technologies that can empower that mission. We have fully scoped out the solutions we want to build and understand the technologies required to build it. In the consortium, we have found seasoned and renowned research and technology partners who have developed their own expertise and own maturity which makes them ideally suited to contribute to the project. Whether it is consortium leadership and legal expertise (De Roos Legal), advanced zero knowledge solutions research and protocol implementation (Universidad Carlos III de Madrid), data analytics and multi-party computation (Partisia), advanced technical development and integration (Parhelium), advertising performance analysis and customer engagement (Publicis Bulgaria), or platform development and strategic contribution, and commercial involvement (Profila), this consortium brings together technical and subject-matter expertise along with an ambitious and potentially world-changing mission brought forward to solve real societal challenges through clever and mature use of existing and emerging technologies into a platform that serves the needs of the EU and its citizens.

The technology maturity is evolving, and this project will propel it forward to a state that is ready to be released to the individuals and brands in the form of a platform, a rich set of features, products and services which can be expanded and improved by the participants in this consortium and new entries in our ecosystem.

Below we further describe the excellence, objectives and ambition of each work package:

1.1.1. WP1: A New Internet Experience

Horizon Digital Decade Contribution – People at The Centre

Digital technologies should protect people's rights, support democracy, and ensure that all digital players act responsibly and safely.

Excellence – Through Design

Through extensive research, prototyping, and alpha testing, we have distilled a fundamental truth: individuals demand privacy and personalisation yet remain indifferent due to the lack of accessible management tools. They recognise the inherent value in their personal data, but lack effective means to capitalise on it. There is a clear willingness to exchange data for value, provided that privacy is not compromised. It is with these insights in mind that we occupy ourselves regarding the new internet's design. How will people learn these new habits of data creation, control, sharing and monetisation? This will not be achieved through deep technologies alone; this will be achieved through brilliant design.

We have for the past few years researched how to develop a new approach to digital relationships and are developing a Beta version of this data experience that places individuals at the centre of their digital experiences with any organisation globally, ensuring empowerment and control within the digital ecosystems they choose to wander in and stimulating mindful attention to the content they want to see.

The objective in this project is to continue the evolution of this people-centric design philosophy by improving on and introducing planned community tested features that incentivise and empower people. This design evolution will ensure the adoption of the platform and the underlying enabling technologies that will empower each EU Citizen.

Innovation and approach

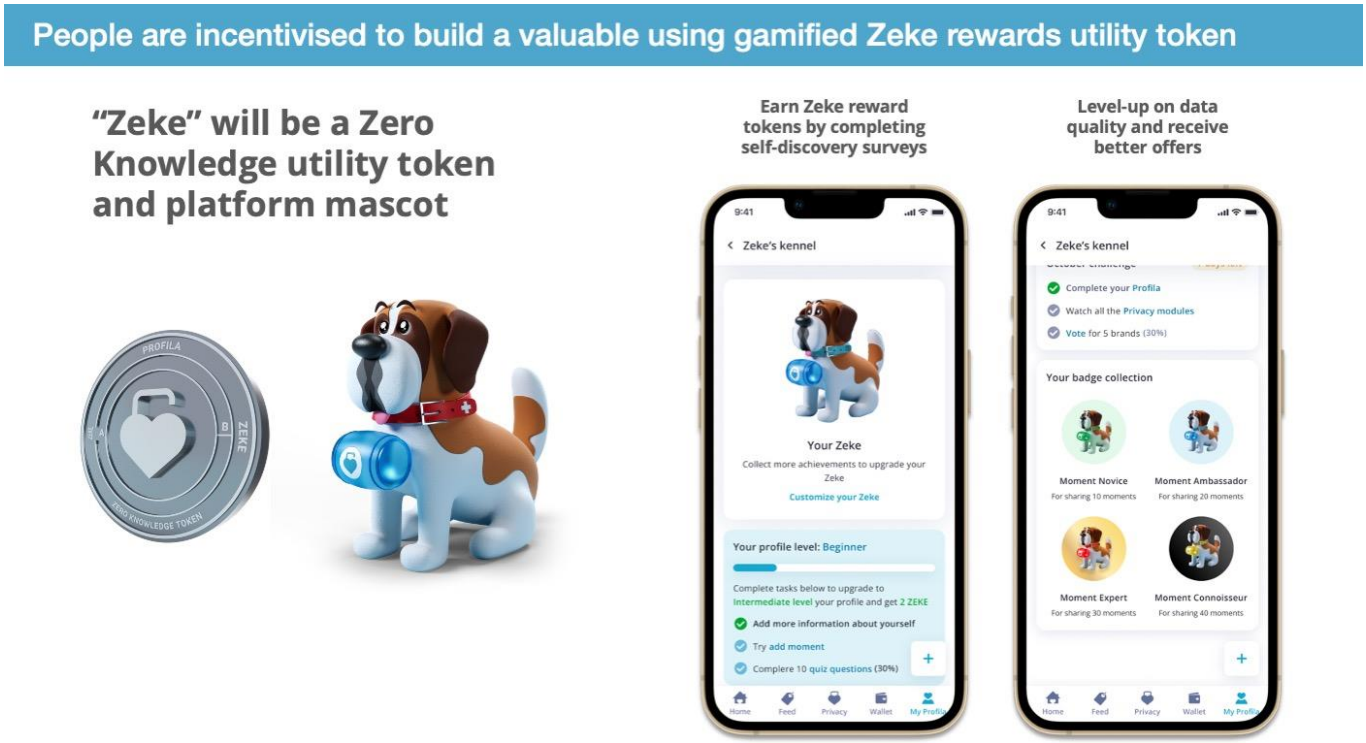
In developing a truly people-centric platform, we have embraced the methodologies of mindful design and have anchored the system in the concept of zero-party data. The mindful design philosophy consists of the following three pillars:

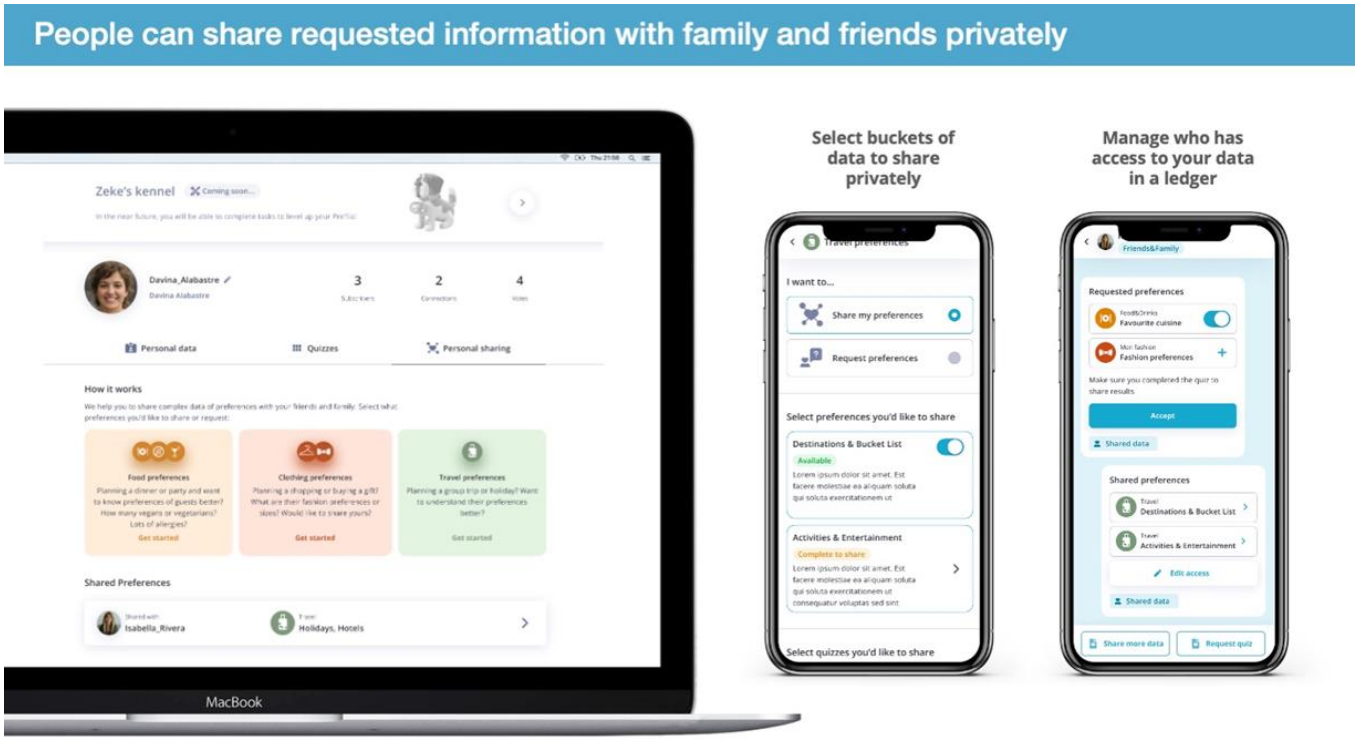
- *Ethical Nudging*. We create an incentive structure that rewards the individual based on their self-interest, not the interests of the platform. This concept of ethical nudging is counter-intuitive to many current platforms but is central to our design thinking and will ensure the proper incentives to keep the platform participants

honest and individuals assured that they have control and agency.

- *Privacy and Transparency*. There needs to be a place in the new digital economy where privacy is paramount. The platform will have complete transparency for every individual concerning who has requested access to parts of their profile and who they have already granted access to (with easy revocability). These tenets will be made obvious in the design and user experience.
- *Control of Data Relationships*. In all interactions on the platform, the individual will have control (for each separate data relationship) as to how often they can be contacted or sent promotional ads and material, and if they want that interaction to be done in a zero-knowledge environment. They will be able to choose, for all data relationship and interactions, whether they are a known individual to the other party or completely anonymous.

The platform will be designed for people and delivered to brands or organisations. Our motivation is to offer brands a new private experience where they can honour their customers' privacy while still delivering personalised services. Importantly though, we have planned to implement multiple person-to-person (peer-to-peer) features to ensure that the value of the platform expands beyond material or business relationships, to those personal and private in nature.





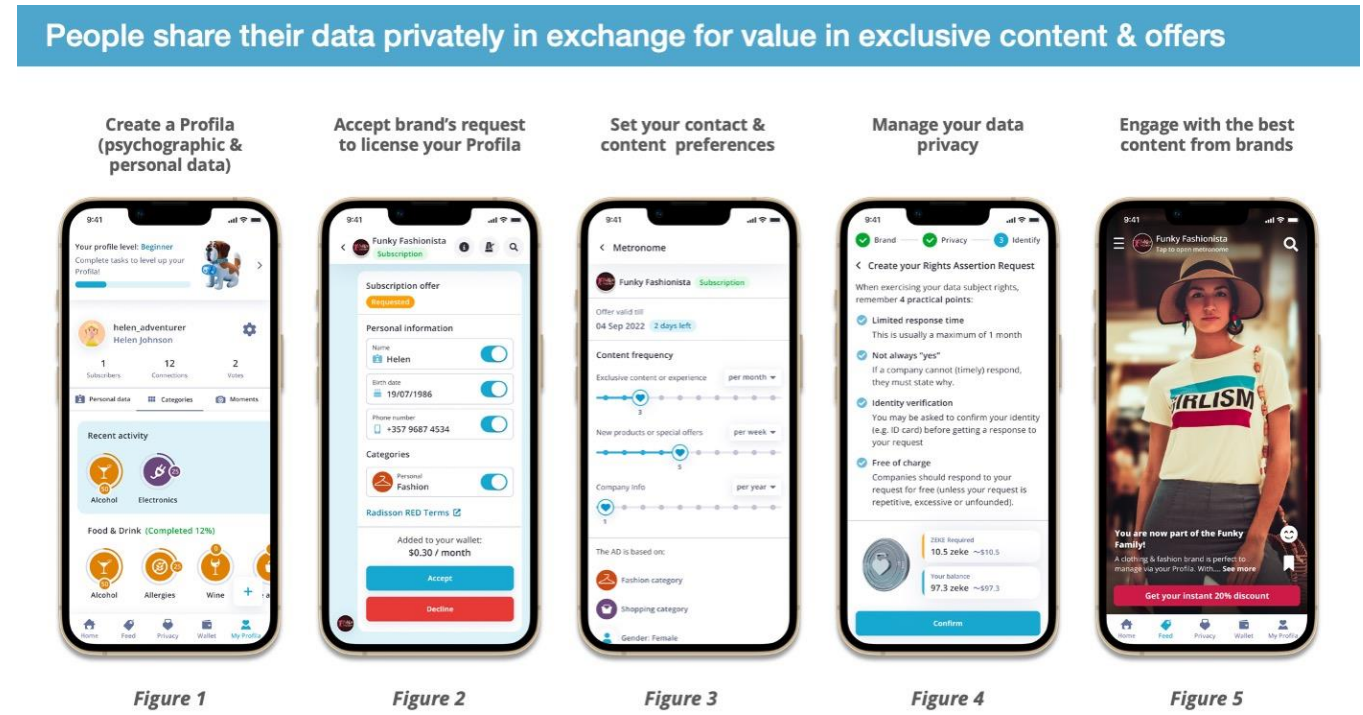


Figure 1 *Figure 2* *Figure 3* *Figure 4* *Figure 5*

Planned features include:

- For individuals:
    - creating a personally identifiable information profile (Figure 1)
    - creating psychographic data profile through self-discovery surveys
    - voting for and connecting to brands as a digital call to action
    - accepting or rejecting a data subscription from a brand (Figure 2)
    - viewing personalised content or adverts from a brand (Figure 5)
    - asserting a privacy right with a brand (Figure 4)

- For brands:
    - subscribing to customers' personal data, for a specific duration and purpose
    - creating anonymous lists of customers and advertising in a privacy-preserving channel with zero tracking
    - creating a data subscription for targeted customers to deliver highly personalised content and advertising.

New features that will be community-tested and implemented include:

- For individuals:
    - creating a Web 3.0 digital ID profile, federated to the EU eID
    - sharing data privately and peer-to-peer with family and friends
    - a personal preference centre to control attention given to brands (Figure 3)
    - a data marketplace for buying signals – placing higher value datasets/leads on sale to predefined brands or the open market.

1.1.2. WP2: A "Profila": A Privacy-Preserving Profile for a New Internet

Horizon Digital Decade Contribution – Safety and Security and Participation

The digital environment should be safe and secure. All users, young and old, should be empowered and protected. Citizens should be able to engage in the democratic process at all levels and have control over their own data.

Excellence – Through Technology

The platform's heart will be dynamic, secure, and private digital profile – branded as an individual's "Profila". It empowers individuals to cultivate a singular online identity that streamlines their internet interactions and the content they engage with. This centralised approach not only simplifies the user experience but also elevates the value derived from digital interactions, thereby energising the digital economy.

Innovation and Approach:

Our technological strategy encompasses:

- *Digital Identities:* through the implementation of Decentralised Identifiers (DIDs) for each Profila, integrating the EU eID to facilitate secure and verified data sharing.
- *Data Spaces:* through the creation of two distinct data spaces using the Solid Flanders Pod project's framework, ensuring user data remains protected within an open-source environment.
- *Multi-party Computation:* through the deployment of multi-party computation techniques to offer organisations privacy-preserving insights, with plans to integrate homomorphic encryption to enhance data security across these spaces.
- *Identity, Decisions, and Payments Blockchain Ledger:* through the development of a blockchain ledger system to chronicle identity verifications, user decisions, and transactions, reinforcing the platform's commitment to transparency and user empowerment.

1.1.2. WP3: A Zero Knowledge Advertising Protocol ("The Cookie Killer")

Horizon Digital Decade Contribution – Freedom of Choice and Sustainability

People should benefit from a fair online environment, be safe from illegal and harmful content, and be empowered when they interact with new and evolving technologies like artificial intelligence. Digital devices should support sustainability and the green transition. People need to know about the environmental impact and energy consumption of their devices.

Excellence – Through Research

An individual's data-sharing choices and preferences should be shared with advertisers and the internet at large, outside of any walled garden.

Innovation and Approach:

In collaboration with Universidad Carlos III de Madrid, Profila has conducted research into Zero Knowledge Advertising, aiming to redefine privacy-preserving methodologies. This initiative strives to replace outdated third-party cookies, setting a precedent for enhanced privacy on the internet. The abstract of that paper states the following:

Zero Knowledge Advertising: a new era of privacy-preserving AdTech solutions

New data protection legislation, along with the social pressure, has encouraged the online advertising industry to propose a novel privacy-preserving advertising solution, such as Brave or Google's Topics. While these pioneering solutions represent an undoubtedly important step towards a more ethical form of targeted advertising, they present some limitations. In this paper, we first systematically identify the limitations of the most promising industrial solutions. Armed with such knowledge, we present a new (simple and efficient) privacy-preserving solution for delivering targeted ads, which combines the benefits of state-of-the-art proposals. To confirm the operational viability of our solution in the current online advertising ecosystem, we have performed extensive simulation experiments assessing that: (1) our solution requires minimal use of the devices' resources (memory and CPU), making it valid for handheld devices running on limited power batteries; and (2) our solution meets the strict timing requirements for the delivery of ads imposed in the online advertising ecosystem. See Annex 1 for the full version of the Zero Knowledge Advertising paper.

These findings were presented at the Crypto Valley Conference (2022) in Zug by representatives of Universidad Carlos III de Madrid and Profila (see Masterclass - A new era of privacy preserving adtech solutions).

1.1.3. WP4: A Better Data and Attention Business Model

Horizon Digital Decade Contribution – Solidarity and Inclusion and Participation

Technology should unite, not divide, people. Everyone should have access to the internet, to digital skills, to digital public services and to fair working conditions. Citizens should be able to engage in the democratic process at all levels and have control over their own data.

Objectives and Relevance:

Our project seeks to establish an equitable business model that benefits individuals and corporations. Our research is geared towards devising compensation mechanisms for individuals' data and attention that honour privacy and data security, aligning with stringent standards like those under the GDPR. The applied business model development is based on business model canvas and value proposition design in alignment with the currently emerging Next Generation Internet (NGI) concept guidelines of the EU. While the main focus is put on developing an attractive business model for the Web 3.0 environment, our efforts also include investigating the emerging standards for Digital Twins, driven by the Web 4.0 and Virtual Worlds initiative of the European Commission. This way we make sure that the business model is already designed in a way that it is prepared for a future in the 3D-spatial web world.

Innovation and Approach:

Our approach pivots from the traditional model of selling personal data. We recognise the inherent risks this poses to privacy and security, as well as the loss of individual autonomy. Therefore, our paradigm is to leverage personal data and attention as currencies in their own right, rewarding individuals with value in the form of services and products. This model ensures compliance with stringent privacy regulations such as the GDPR, fostering a business ecosystem that prioritises and respects user consent and data rights. We will furthermore investigate if an alignment of Digital Twins with the standards arising from the very latest Web 4.0 and Virtual Worlds approach can enhance user experience and elaborate related suggestions. This will include, for example, research related to future improvements of the business model with regards to applying gamification, enhanced "tokenomics" and integration into the 3D-business-worlds of the future. This way, rational privacy improvements might additionally benefit from the 'fun-factors' delivered by the 3D-spatial web world.

1.1.4. WP5: A Privacy by Design Platform

Horizon Digital Decade Contribution – People at the Centre

Digital technologies should protect people's rights, support democracy, and ensure that all digital players act responsibly and safely. The EU promotes these values across the world.

Excellence – Through Privacy

In partnership with law firm De Roos Advocaten, experts in data protection law, we are validating our platform's GDPR compliance capabilities and accountability. By integrating their legal expertise, we aim to perform comprehensive Privacy Impact Assessments (PIAs),meticulous data mapping, and take other steps necessary under the GDPR and other (e-)privacy related legislation. This collaboration is vital as we need to confirm the 'privacy compliance' part of our technology.

Innovation and Approach:

De Roos is an expert in privacy law and related fields of law, such as digital, data and AI regulations. There innovative character is showed by e.g., the fact that they already have to operating spin-off companies (one in software, one in legal design). The De Roos involvement will ensure the privacy-by-design approach by confirming that all principles of the GDPR are fully designed into the product, including fairness, transparency and control, data minimization and storage limitation.

1.1.5. WP6: A Sandbox for Enterprises to Learn

Horizon Digital Decade Contribution – People at the Centre

Digital technologies should protect people's rights, support democracy, and ensure that all digital players act responsibly and safely.

Objectives and Relevance:

The objective is to foster a digital transformation by launching a Business Launch Platform focused on the burgeoning Web 3.0 landscape. Aimed at encouraging early enterprise engagement, the platform is designed with a tripartite structure: (1) Think Tank and Expert Community to facilitate strategic discussions; (2) Knowledge Management and Training hub to educate and empower users; and (3) Proof-of-Concept and Value Proposition Sandbox to test and validate innovative ideas. This layered strategy is poised to bridge significant gaps in the digital domain by prioritising identity security and data privacy and by efforts to investigate integration pathways for the various private sector Web 3.0 privacy applications with the emerging European public sector solutions like EUDI-Wallets and alike.

Innovation and Approach:

The initiative is led by Heinz Gassner, a professional with over 30 years of expertise in automating and digitally transforming the manufacturing industry. His leadership is instrumental in orchestrating the Think Tank and Expert Community, which serves as a crucible for discourse on digital identity and privacy. This community will not only delve into the intricacies of digital identity within the scope of the European Digital Decade 2030 initiative but will also extend its dialogue to incorporate related projects, thereby shaping the future of Europe's digital landscape.

#§PRJ-OBJ-PO§#

1.1.6. WP7: Project and Programme Management

Objectives and Relevance:

The fundamental objective of this work package is to meticulously implement project management best practices, ensuring the delivery of a project that not only aligns with but also exemplifies the high standards set by the Horizon 2020 programme.

Innovation and Approach:
Michiel Van Roey is an EU-qualified business lawyer and a seasoned technology entrepreneur with a track record

of leading international teams and managing international research and development projects, akin to the one outlined in this application. As the former General Counsel at Cisco Benelux, he led a team of five lawyers and managed the region, which generated $2 billion USD in sales. Notably, he spearheaded Cisco's Innovation Office in Paris.

In addition to his corporate achievements, Michiel serves as the project manager for an Innosuisse-funded research project, titled "50446.1 IP-ICT INNOSUISSE - P2Sr Profila Privacy Simplified Reloaded". This project, aimed at developing an open-smart knowledge base on Swiss privacy policies and legislation, simplifies consumer access to legal knowledge and expertise. Details can be found at Aramis Project. Throughout this two-year research endeavour, Michiel is coordinating the efforts of five researchers from the Lucerne University of Applied Sciences (HSLU), collaborating closely with Profila's business and technical teams.

At De Roos, Michiel is co-leading this project with Annemarie Bloemen. While Annemarie concentrates on privacy/GDPR-related legal aspects, Michiel oversees the administrative sector of the project management. His comprehensive experience and established rapport with all consortium partners position him exceptionally well to lead this intricate and significant work.

Shawn Jensen is an accomplished executive with a wealth of experience in fostering innovation and driving revenue growth in the enterprise sector. Holding a master's degree in Leading Innovation and Change, Shawn has been a pivotal figure in the launch and development of various new business models. His career includes significant tenures at Vodafone Global Enterprise (VGE), where he held senior management roles and excelled as the Head of Product - Connectivity and the Head of Customer Pre-sales and Service for the Middle East and Africa.

During his time at VGE, Shawn was instrumental in establishing operations for design, delivery, and service management across Africa, significantly contributing to regional revenue growth through the adoption of best practices and effective leadership of diverse, multicultural teams. His skills were further showcased in his role as the Solution Architecture Regional Lead for VGE in Central and Southern Europe. Here, he was responsible for teams tasked with designing global telecommunication solutions tailored to meet the needs of enterprise customers.

Currently, at Profila, Shawn is at the forefront of developing a cutting-edge Web 3.0 personal data relationship and permission marketing platform. This innovative platform is designed to offer value to individuals and brands alike, facilitating private communication and content channels. Shawn's proven track record in leading complex telecommunications projects, combined with his expertise in innovation and revenue generation, positions him as a valuable asset to any organisation, particularly in his role leading the technical delivery of the Horizon project.

1.2 Methodology #@CON-MET-CM@# #@COM-PLE-CP@#

Overall methodology

This project will adopt a robust and interdisciplinary approach to achieve its ambitious objectives. The expertise of the different partners in computer science, cybersecurity, blockchain, marketing and communications, and legal areas will be combined to ensure the success of the project and excellent scientific, technological and innovation outcomes. By incorporating the following methodologies, the project aims to develop innovative solutions with a focus on technical excellence, user experience, legal compliance, and broad applicability, while also addressing important societal and ethical aspects.

- *Technical Focus:* With a strong emphasis on computer science, research and design, the project will develop tools for system monitoring and data security.
- *Intelligence Information Analysis:* The project involves analysing and improving existing AdTech solutions for better data understanding and application.
- *User Interface Development:* Focus on creating user-friendly interfaces for the project's solutions, combining data handling with easy-to-use design.
- *Legal and Standardisation Integration:* The project not only develops new tools but also ensures legal compliance and adoption by incorporating legal expertise and standardisation knowledge.
- *Real-world Testing:* Deploying a Sandbox for enterprises to test technologies in real use case scenarios, especially in real time bidding advertising.
- *Industry Collaboration:* Work with industry partners and agencies to test solutions through the Sandbox and gather feedback, ensuring practical applicability and adoption.

International Research Activities

Members of the consortium will bring into the project previous research efforts which will directly contribute to the scope of this proposal, including zero knowledge advertising, the value of zero-party data and practical research about launching a platform to key audiences.

Universidad Carlos III de Madrid Research

- Zero Knowledge Advertising: a new era of privacy-preserving AdTech solutions (in collaboration with Profila)
- González-Cabañas, José, Ángel Cuevas, Rubén Cuevas, Juan López-Fernández, and David García. "Unique on Facebook: formulation and evidence of (nano) targeting individual users with non-PII data." In Proceedings of the 21st ACM Internet Measurement Conference, pp. 464-479. 2021.
- Cabañas, J.G., Cuevas, Á., Arrate, A. and Cuevas, R., 2020. Does Facebook use sensitive data for advertising purposes? Communications of the ACM, 64(1), pp.62-69.
- Callejo, P., Pastor, A., Cuevas, R. and Cuevas, Á., 2019, December. Q-Tag: A transparent solution to measure ads viewability rate in online advertising campaigns. In Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies (pp. 151-157).
- Iordanou, Costas, Nicolas Kourtellis, Juan Miguel Carrascosa, Claudio Soriente, Ruben Cuevas, and Nikolaos Laoutaris. "Beyond content analysis: Detecting targeted ads via distributed counting." In Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies, pp. 110-122. 2019.
- Cuevas, A., Cuevas, R., Aparicio, R. and Gonzalez, J., 2017. Fdvt: Data valuation tool for Facebook users. In Proceedings of the Conference on Human Factors in Computing Systems (CHI'17).

Profila Research

- PRIMARY RESEARCH: NLP for Privacy and Customer's Education (Ongoing)
  Natural Language Processing for Information Resources Suggestions and Expert Finder Systems (Innosuisse Grant Funded)
- Master Thesis - Privacy vs. Benefit. (with Hochschule Luzern)
  An Analysis on What Items of Personal Data Millennials living in the German-speaking part of Switzerland would be Willing to Share for a Desired Benefit.
- Profila Alpha Trials - 2020
  Findings from Consumer Research pre and post Profila App alpha trials conducted in Central Switzerland involving 5 commercial companies and 70 individual participants.
- Profila Marketing Campaign for Gen Z (with Zurich International School)
  Understand social media usage of target audience of pre-college Gen Z and their relationship with brands and personal data sharing
- Zero Party Data Collection and Usage (with Hochschule Luzern)
  How Zero-Party Data Could Change Swiss Business-to-Consumer (B2C) Companies' Marketing Practices and Strategies.
- Zero-Party Data in the Tourism Industry (with Hochschule Luzern)
  Major Online Business and Marketing - Applied Research Project

Partisia Research

Partisia participates in numerous research and R&D project with universities and companies to form the starting point for new innovative solutions and businesses. As a spin-off from internationally ground-breaking research results – R&D is an inherent part of Partisia's DNA. Partisia is pioneer in commercial use of zero-knowledge computation such as secure MultiParty Computation (MPC) and the ownership include world-leading researchers and experts in advanced cryptography. Hereby, the team ensures the shortest way from the design of cryptographic protocols to commercially viable software solutions.

Partisia Blockchain is built on almost four decades of academic research into cryptography, computer science, and economics. Below you can find reference to the research papers per researcher, diving into the theoretical

underpinnings of Partisia's revolutionary technology, with the main research papers from Partisia that are relevant for this application being the following:

Main research papers:

- Balancing Privacy and Accountability in Blockchain Identity Management - Part of the Lecture Notes in Computer Science book series (LNSC, volume 12704)
- Minimising Setup in Broadcast-Optimal Two Round {MPC} - Part of the Lecture Notes in Computer Science book series (LNCS, volume 14005)
- Fast Fully Secure Multi-Party Computation over Any Ring with Two-Thirds Honest Majority CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security

Link to exhaustive research from Partisia can be found here https://partisiablockchain.com/category/research/.

Social sciences/humanities

In line with the project's overall direction, this project builds upon a proper combination of SSH (law, ethics, marketing and communications) and STEM disciplines (science, technology, engineering, and mathematics) to create novel, simple, and scalable solutions. This will provide a toolbox that makes realising other policy goals (competitiveness of the European economy being the most important) possible. The integration of SSH and STEM is reflected in the work package structure and how inputs will inform the technical work packages to ensure that the technical and non-technical requirements are fulfilled throughout the entire innovation process. Moreover, De Roos will also ensure that, insofar as practicable, all legal and ethical aspects are considered since the design and transparency principles are respected. De Roos acts as the legal partner for this project and will oversight and provide input to all other consortium members on the legal, ethical and social requirements, throughout the research and innovation process.

Gender dimension

While the list of stakeholders in this proposal are wide and varied, the core of the project is to serve each individual human being in the EU. All of us, to some extent or another, have an online life; whether it is through social media, shopping online, to simply navigating the internet for pleasure, information, or curiosity. We all will benefit from a new environment where our activity on the internet is more protected from prying eyes, that our sentiments and preferences are ours to have and to hold, and we maintain a freedom of association where we can include or exclude anyone else from communicating with us as we see fit.

With that in mind, we acknowledge and appreciate that the internet can be an especially fraught place for women, whether it takes the form of simple harassment or more dangerous aspects. When we conceived this project, we understood that those most vulnerable will receive even more benefit from being the owner of their personal data, be able to conduct their affairs online in privacy when they so choose, and to have the control over who can interact with them online. Everyone will benefit, but some require and deserve that benefit more than others.

Although gender balance within the consortium's team is not a requirement of the application, we are proud that on top of the geographic diversity we enjoy in our consortium as our partners stretch across the EU, we also have excellent gender representation across all disciplines, from our legal partner, researchers, commercial partners, and designers. A project that will benefit each individual is made better by representing all kinds of individuals. We know the outcome of our project will also be better because of our approach.

Open science practices

Our project is committed to Open Science principle and will comply with all mandatory Open Science practices in Horizon Europe regulated under the Article 17 of the HE General MGA v1.0 and related guidelines. Additionally, we will implement several recommended Open Science practices as an integral part of our project, as all project objectives heavily rely on open collaboration, diffusion of knowledge, sharing of data, and co-creation of technology solutions. Our project's methodology and scientific approach will foster, as early as is practical the key basis being 'as open as possible, as closed as necessary', open cooperative work and systematic sharing of knowledge and tools. Aligned with the dual ambition of ensuring excellence and impact of public investment in the Action, while safeguarding the EU's interests, the consortium will adopt several Open Science practices, namely Open Access, Open Data, Open Source, Research Ethics, Integrity, and Reproducibility, and End User Engagement.

Open Access
The project's participants will ensure immediate Open Access to the peer-reviewed scientific publications relating to the project results (while retaining sufficient IP Rights to comply with Open Access requirements). This will be done no later than the publication date and through trusted repositories like Open Research Europe, and arXiv (Technical content) under a CC-BY. Publication will be added to the project website and shared with networks of related research communities and new versions of manuscripts will be added if necessary. Sufficient IP Rights to comply with open science requirements will be retained and Directory of open access journals (DOAJ) will be followed for quality assurance. We will choose open access peer-reviewed journals with CC-BY license.

Open Data
The project's participants will manage all digital research data (and metadata) responsibly and in line with the FAIR principles. The data will be as open as possible (to ensure reproducibility and reuse) and as closed as necessary (to allow for the protection of results). We will establish and regularly update a Data Management Plan (DMP) for the generated and/or collected data. As soon as possible and within the deadlines set out in the project plan, we will deposit the research data in a trusted repository (e.g., Open Research Europe) and ensure open access to the data under a license that allows for a wide reuse (e.g., CC BY). We will ensure output management beyond research data by making all guidelines, recommendations, requirements, frameworks, and best practice findings public.

Open Source
The models, algorithms, designs, and software developed in this project will primarily and as much as possible be released in open source, with some exemptions to safeguard partners' commercial interests. To this end, a version of the open-source technologies developed will be published on open repositories (e.g., GitHub, GitLab, Joinup) with open licenses. We commit to follow best practice for software documentation as a key to the success of software adoption as well.

Research Ethics, Integrity, and Reproducibility
All research and innovation conducted during this project will adhere to commonly agreed high scientific standards of research ethics, integrity, and reproducibility. The researchers will follow and promote the key principles of ethics in research (honesty, integrity, objectivity, openness, respect for intellectual property, etc.) and adopt the European Code of Conduct for Research Integrity.

End User Engagement
The technologies deployed will be tailored to end-users, and they will be involved in all development phases (from the design, throughout the development and integrations, to the final demonstration, evaluation, adoption, and promotion). This is precisely why one of the six consortium partners – Publicis Bulgaria – is an advertising agency with a considerable portfolio of brands who are interested to test the platform developed under this application, with their real customers. We will therefore be able to engage with real world users during the sandbox work package.

Data management and management of other research outputs
A sound Research Data Management (RDM), in line with FAIR principles for all data, will be followed, covering all the relevant dimensions (e.g., data collection or acquisition, organisation, storage, security, quality assurance, provision of persistent identifiers, sharing, licensing). A full Data Management Plan (DMP), following the Horizon Europe template, will be submitted by month 6 of the project, ensuring responsible management of research outputs. The DMP, which will be further revised towards the end of the project, will: (i) duly justify any data excluded from open access; (ii) detail all the assets and material underlying data collection and analysis (data types, estimated size, association to specific research, standards and metadata used to structure the data); (iii) outline all aspects of the research data lifecycle (e.g., adequate provisions for data curation and organisation, its security, storage and preservation, rules and provisions for its access/sharing, and eventual deletion, both during and after the project).

Types of data / research outputs
In the DMP generated datasets will be sufficiently described including their scientific focus. We will distinguish between existing datasets under exclusive control of organisations; or else encrypted datasets sets shared between partners in encrypted form over such encrypted data which are not possible to share externally; and general datasets with no personal data which may be shared for further research under certain conditions. Other key research outputs refer both to scientific and technical knowledge generated, and to the interplay of human and societal (SSH research) outcomes with technological aspects and challenges which will be subject to wider dissemination through publications and other materials adapted to different audiences.

Findability of data/research outputs
Open access publications and open research data will be deposited in a trusted repository (preference is on Open Research Platform) using open licenses, with respect to beneficiaries/authors' legitimate interests and IP rights. In the case of research data, the deposit will take place after adequate processing and quality control have taken place, providing value and context to the data, at the latest by the end of the project (when data cannot be made open, the deposit can focus on making metadata available to ease findability).

Accessibility of data / research outputs
As explained in the previous section, and for data which are not under exceptions such as special categories of data under GDPR, open access to generated research data will be enabled through open data arrangements and where applicable (e.g., limited access for data verification purposes by authorised stakeholders) through conditioned data access and sharing agreements (e.g., to associated partners or specific groups). IP Rights management and (co-ownership rights considerations as established between consortium members in the consortium agreement (among other relevant provisions such as licensing agreements or approval processes) and following Art. 16 of Model Grant Agreement will be applied as relevant in each case.

Interoperability of data / research outputs
Common community standards, including relevant standardised metadata frameworks (e.g., HL7), formats and vocabularies will be assessed and selected in the initial phase of the project to reference metadata and to maximise interoperability of data and research outputs. On a technical level, whenever possible, APIs will be designed with the goal of maximising interoperability for input/output data produced by the tools made available to external stakeholders.

Reusability of data / research outputs
To the extent beneficiaries/authors' legitimate interests and IP rights are ensured, access to deposited data in a trusted repository will be granted under the latest available version of CC-BY (or a licence with equivalent rights) and CC0 for metadata (i.e., machine-actionable). Data will include all relevant information on datasets (e.g., description, date of deposit, author(s), venue, and embargo), project (e.g., funding, name, acronym and number, licensing terms, the authors involved, and, if possible, for their organisations).

Curation and storage/preservation costs
Data curation and preservation will follow a specific strategy considering aspects such as the nature of the different types of data and research outputs identified and described in the DMP, quality requirements for their reusability and distinguishing those research data and results that may remain usable and valuable for longer time periods.

#§CON-MET-CM§# #§COM-PLE-CP§# #§REL-EVA-RE§#

2. Impact #@IMP-ACT-IA@#

2.1 Project's pathways towards impact

Project impact

As outlined in the description on the United Nations website on the Sustainable Development Goals for goal 9, more than half of the world's population is now online and businesses have increasingly digitalised their products and services. COVID-19 only increased people's use of the internet for access to essential goods and services, healthcare, and education.

More people thus interact and exchange their (personal) information with companies, organisations, healthcare providers, schools, and even governments over the internet. This is all part of the 4th industrial revolution, which is a data-driven economy with new business models. However, whereas companies and organisations have the means to take part in the data driven economy, people often lack the same resources and knowledge. As indicated on the website of the World Economic Forum, the 4th industrial revolution should be about more than just technology-driven change but should be seen as an opportunity to help everyone, harness converging technologies in order to create an inclusive, human-cantered future.

It is in this space that our platform plays a crucial part. It will help brands and organisations transform to a person-centric digital customer relationship, with a new private channel to advertise to and communicate with their

customers, surveillance-free; while providing consumers with the resources and knowledge to keep up with this digital revolution. It will be a simple tool for individuals to learn about and manage personal data, enforce privacy rights, monitor relationships with brands; and obtain compensation for data shared.

In order to further explain how the project's results are expected to make a difference in terms of impact, beyond the immediate scope and duration of the project, and who will benefit from this impact, we first need to elaborate further on the problem that our project will tackle.

Introduction – the privacy, identity and digital trust problem

Today, there is a clear privacy problem on the internet, considering internet users have almost no control over the collection and use of their personal data online. Brands have collected their personal data, and they decide – at their own discretion – how they use your personal data for their benefit. You interact with digital services and purchase products from companies or "brands" globally. With each interaction you directly share personal data which is used for a certain purpose such as offering you a product and servicing you as a customer. But what can you do if a brand uses your data against your will?

In addition, the internet has no "identity layer", namely it is not possible to know who is behind a certain social media account, who is the owner of a certain website, or who is selling you products and services. The only identity that exists is centralised identity, where a brand collects a part of your identity (e.g., username, password, credit card details) when you use their products. Today's centralised identity on the "Web 2.0" version of the internet gives rise to several issues, from difficult identity verification to data breaches and limited interoperability.

Finally, a large part of the time you spend online (social media & websites), you are being subjected to online advertising. The Ad-Tech market touches billions of consumers and it is reliant on collecting and sharing a large amount of people's personal data. Your personal data – along with the data of billions of other internet users – gets shared with and used by numerous companies for their (commercial) benefit. There is a clear lack of privacy, identity and digital trust on today's internet, which our consortium intends to tackle and have an impact on.

More people demand more control and are willing to take action to take back ownership of their digital lives but are lacking the tools or know-how to make this happen and give brands clear instructions about the frequency of interaction, the channel of preference, and the content of choice. There is a clear need to level the playing field, to bring people on the same level of technical maturity as brands, to make this exchange of information and content consumer-consenting, and two-directional.

A recent consumer privacy survey conducted by Cisco Systems[1]– interviewing 2,600 adult respondents in 12 of the world's largest economies (five in Europe, four in Asia Pacific, and three in the Americas) – shows that people increasingly care about their personal data and want to actively take action to protect it. The study showed that people are looking to take action to protect their data; with 84% of people who "care"; 80% of people who are "willing to act", and 48% of people who have already "acted", for example by switching companies or providers based on their data policies or data sharing practices.

The impact will be both economic and societal, as it could (1) enhance the digital privacy of +1 billion internet users (children and adults), while (2) the increased trust between people and brands will stimulate the digital economy as more trusted interaction and transactions will occur, all while (3) reducing the cost of add fraud and (4) making digital advertising greener and more sustainable.

Long term impact no 1 – increase digital privacy of 1 billion internet users
That is where the consortium's platform steps in, by providing people with the tools to control their data and their experiences with brands, while maintaining their privacy and identity.

Long term impact no 2 – increase digital commerce by enhanced trust between people and brands
Once there is trust between people and brands, and if brands would (only) serve people with adverts that are based on their personal profile and preferences, we believe there will be a higher conversation rate and increase in spend.

[1] Cisco Survey, https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf

Long term impact no 3 – reduced ad fraud
Brands will only be able to serve an advert to an identified individual, who can only make one single account that is verified (KYC), reducing ad fraud to nearly 0% from the current 40%.

Long term impact no 4 – sustainable marketing
The project impact of greener and sustainable marketing also falls under SDG goals 7 (affordable and clean energy), 12 (responsible consumption and production)

Energy is today the most critical environmental challenge. The amount of carbon emissions contributing to climate change is significantly influenced by both the production and consumption of energy. Measuring and reducing the energy consumption of services is a crucial step toward reducing adverse environmental effects caused by carbon emissions. Millions of websites rely on online advertisements to generate revenue, with most websites earning most or all of their revenues from ads. As a result, hundreds of billions of online ads are delivered daily to internet users to be rendered in their browsers. Both the delivery and rendering of each ad consume energy.

Since the advent of the internet in the early 1990s, the Information and Communication Technologies (ICT) sector has become a major driver of developed economies as well as a factor contributing to the increase in global energy consumption. Depending on the source, the total energy consumption of the Internet is approximated to be between 5% and 15% of total global energy consumption, that is around 416.2 TWh per year. This percentage is projected to rise sharply in the coming years. Online advertising is one of the main sources of revenue supporting the operation of the commercial Internet. Millions of websites, social media platforms, mobile apps, video platforms, etc, rely on online advertisements as their main source of revenue. As a result, each day, hundreds of billions of online ads are delivered to Internet users to be rendered by their devices. Indeed, online advertising is a $450 billion per year industry with an inter-annual growth of 35.4% between 2020 and 2021, according to the IAB's most recent Internet Advertising Revenue Report of 2021.

It is exactly here where the consortium's new consent-based advertising model is revolutionary. Because people will be able to use the platform to limit the number of ads they see and directly communicate the frequency of ads to the companies they like to engage with, a company will only send an advert when it is relevant. This consent-based advertising model will drastically reduce the number of (unwanted) ads that are shown today, thereby also drastically reducing the energy consumption of the online advertising industry.

2.1.1. WP1: A New Internet Experience

Key Impact Pathways (KIPs):

Our project directly aligns with the EU's strategic objectives by enabling individuals to actively manage their digital identities and data privacy, thus contributing to the creation of a secure, privacy-respecting digital market. By leveraging zero-party data, we will foster an environment where personalisation does not come at the cost of privacy, supporting the EU's goals for a sustainable and competitive digital economy.

Project's Pathways towards Impact:

We anticipate that the adoption of our platform will lead to an increase in digital literacy regarding data management and privacy, empowering EU citizens to engage with digital services on their terms. This empowerment will translate into a more dynamic and trustworthy digital market.

Measures to maximise impact - Dissemination, exploitation, and communication #@COM-DIS-VIS-CDV@#

To maximise our project's impact, we will focus on community engagement and the rollout of features that incentivise mindful data-sharing and control. This approach not only respects individual privacy but also provides a model for businesses to interact with customers in a more ethical and transparent manner.

#§COM-DIS-VIS-CDV§#

2.2.1 WP2: A "Profila": A Privacy-Preserving Profile for a New Internet

Key Impact Pathways (KIPs):

- Digital Autonomy: By enabling users to manage their own Profila using DIDs, the project aligns with the EU's goal of fostering digital autonomy and sovereignty.
- Innovation in Data Management: The integration of advanced data spaces and multi-party computation signifies a leap in data management and privacy, promoting innovative practices that can be adopted EU-wide.
- Strengthening Data Security: The implementation of homomorphic encryption and a blockchain ledger for identity and transactions exemplifies the EU's pursuit of secure and transparent digital infrastructures.

Project's Pathways towards Impact:

- User Empowerment: This project positions users at the helm of their digital experiences, enhancing their control and privacy.
- Economic Growth: By improving the quality of user attention and interactions, the project aims to stimulate the digital economy, aligning with the EU's Digital Single Market strategy.
- Policy Contribution: The platform's design reflects the EU's regulations like GDPR, offering a model for compliant digital service development.

Maximising Impact:

- Community Engagement: Through the Profila platform, we aim to maximise the impact by fostering a community-centric approach, ensuring that digital identity solutions are widely adopted and valued.
- Collaborative Expansion: The project will engage with EU partners to expand the reach and integration of the platform, thus maximising its impact on the EU digital economy.

2.3.1 WP3: A Zero Knowledge Advertising Protocol: The Cookie Killer

Key Impact Pathways (KIPs):

- Advancement of privacy-enhancing technologies, aligning with the EU's focus on strengthening digital rights and autonomy.
- Contribution to the development of user-centric data economy models within the EU's framework for a trustworthy digital market.

Project's Pathways towards Impact:

- Deployment of the Zero Knowledge Advertising protocol, contributing to the EU's objectives of fostering secure, private digital spaces.
- Promotion of GDPR compliance and eID integration, reinforcing the EU's stance on digital identity and privacy.

Maximising Impact:

- Encouraging wide-scale adoption of the Zero Knowledge Advertising protocol across the EU, potentially influencing global digital advertising norms.
- Pioneering the next wave of internet privacy standards, potentially guiding future EU policies and digital economy strategies.
-

2.4.1 WP4: A Better Data and Attention Business Model

Key Impact Pathways (KIPs):

The project aims to empower individuals with data control, ensuring equitable treatment and minimising the potential for misuse of data, thus contributing positively to social dynamics, and mitigating issues such as misinformation.

Project's Pathways towards Impact:

Our objective is to revolutionise data utilisation practices, emphasising fair compensation for data sharing to mitigate risks associated with data privacy breaches and psychological stress from invasive data practices.

Maximising Impact:

The goal is to foster a trusted environment demonstrating that data can be leveraged ethically and responsibly, with a focus on creating value for individuals, thereby addressing economic disparities in the digital data realm.

2.5.1 WP5: A Privacy by Design Platform

Key Impact Pathways (KIPs):

Our initiative fortifies Horizon Europe's vision by establishing a secure and private digital landscape, bolstering societal confidence and economic stability through stringent privacy measures.

Project's Pathways towards Impact:

Executing PIAs and extensive data mapping are pivotal for GDPR compliance, ensuring the highest standards of data privacy and establishing our platform as a trusted medium for ethical data sharing.

Maximising Impact:

The completed platform aims to set a new standard for privacy compliance, demonstrating proactive risk mitigation and fostering an environment where personal data is treated with the highest integrity, thereby strengthening the digital economy's trust infrastructure.

2.6.1 WP6: A Sandbox for Enterprise to Learn

Key Impact Pathways (KIPs):

The Proof-of-Concept and Value Proposition Sandbox layer focuses on ideation and the creation of PoCs to demonstrate feasibility and business value, providing a framework for corporate clients to engage with the platform without significant budget requirements. This layer is crucial for translating desire into action and moving forward in the innovation pipeline.

Project's Pathways Towards Impact:

The Think Tank and Expert Community layer is dedicated to reaching senior decision-makers with the aim of addressing the strategic implications of Web 3.0 for businesses. By providing a News Radar, this layer aims to keep the community updated with interdisciplinary insights and foster a deeper understanding of Web 3.0's business value propositions.

Maximising Impact:

The Knowledge Management and Training layer is designed to deepen interest and motivate engagement with practical implementation ideas. This includes the creation of a Navigator tool for self-study and customisable learning journeys, as well as a Risk and Opportunity Radar tool to visualise risks and opportunities.

Potential barriers to achieve desired outcomes and impact

We do not consider regulations to be a disadvantage for the desired outcomes and impact of this project, considering regulations are actually making it possible. Numerous new data privacy, e-privacy and e-commerce regulations have

been adopted that condemn today's digital privacy (mal)practices and call for a solution such as the one described by this consortium.

What could delay the desired outcome would be that the large social media players and search engines keep on supporting the use of third-party cookies and surveillance-based marketing, and that regulators – notwithstanding the powers granted to them by novel (privacy) regulations – refuse to act sufficiently hard against these old practices. However, considering the fines that were given to such players in recent years for failure to comply with GDPR's obligations on transparency, information requirements, informed consent and data subject rights, we believe even regulators are acting appropriately for us to achieve our goals.

Plan for dissemination measures

Brand Partnerships for Dissemination: Partnering with well-known brands allows for leveraging their extensive reach to educate their customer base about the platform's advantages. Collaborative campaigns, joint promotions, or co-branded content can effectively convey the platform's benefits to a wider audience.

Communication Through Educational Institutions and Agencies: Utilising academic institutions and marketing agencies provides avenues for sharing the platform's value proposition and operational mechanisms. This involves workshops, seminars, or educational materials designed specifically for these audiences, emphasising the platform's significance in the digital landscape.

Targeted B2B Messaging: Crafting tailored messages for business partners highlights the platform as a viable alternative to conventional advertising models. Focusing on the platform's unique features and advantages for businesses, such as enhanced targeting or improved ROI, can attract B2B interest.

Direct-to-Consumer Outreach: Engaging directly with consumers is vital for informing them about how the platform empowers them to manage their data and extract greater value from their online experiences. This could involve social media campaigns, educational content, or interactive events aimed at educating consumers about their control over data and the benefits of utilising the platform.

Management of intellectual property

Under the guidance of Michiel Van Roey, technology and intellectual property (IP) lawyer with more than 10 years of experience in technology transfer contracting at the European Organisation for Nuclear Research (CERN), the University of Ghent, Belgium and Cisco Systems innovation office in Paris, the consortium team members will ensure the execution of the proposed commercialisation strategy, firmly supported by a robust Knowledge Management and Intellectual Property Rights (IPR) Strategy, as outlined below and later on detailed in the consortium agreement – DESCA ("CA").

Access Rights

Collaborating members within the consortium commit to granting each other equitable access to each other's Background IP and project outcomes necessary for seamless project execution. Specifics concerning IP ownership and access among project partners, crucial for project execution, will be outlined in the CA before the project commencement. Throughout the project duration, management of these aspects will be overseen by Michiel Van Roey as admin project manager lead for this consortium.

Confidentiality

Throughout the project and beyond (as specified in the CA), all partners are bound to maintain confidentiality of disclosed data identified as such at the time of disclosure. Partners have a 15-day window to formally declare disclosed data as confidential. Disclosure to third parties will strictly adhere to a 'need-to-know' basis, managed by Michiel Van Roey as admin project manager lead for this consortium, ensuring alignment with confidentiality stipulations listed in the IPR log.

Innovation Management

Spearheaded by Michiel Van Roey as admin project manager lead for this consortium, this function aims to promote and safeguard exploitable results generated during the project's lifespan. Ownership of any IP results resulting from specific work within the project will belong to the partner conducting that work. In cases of joint creation or

inventions involving multiple partners, joint ownership will apply. Such agreements and ownership specifics will be documented in the IPR log by Michiel Van Roey. The management of IP results will be outlined in the CA, and subsequent agreements might be established for asset exploitation post-Grant Agreement. All project-produced outcomes will be catalogued and reported in exploitation deliverables, while the IPR log will maintain records of components and their ownership to facilitate conflict resolution and maintain clarity on project IPR status.

Patents

The consortium plans to seek patents wherever feasible. The guiding policy is 'Protect knowledge first (generate IPR), then publish (disseminate results)'. Each participant bears responsibility for patent filings when appropriate. In cases where patents derive from shared know-how, ownership and associated costs will be evenly distributed among contributing parties.

Knowledge Management and Protection

The consortium is set to deliver various innovations in the form of techniques and software components, with ownership resting with the producing partner. Owners of IP produced will take effective measures to protect it, declaring the IP and associated rights in the IPR log. Dissemination or exploitation of project-produced knowledge must align with protection measures and requires consent Michiel Van Roey as admin project manager lead for this consortium.

Additionally, a substantial amount of information and data within the consortium will be attributed to recipients involved in third-party projects. Each third party will undertake responsibility for safeguarding intellectual property arising from the project. Generally, IP concerning knowledge, data, and results from beneficiary projects will remain with the beneficiaries. Consideration will also be given to dissemination and communication of results, with confidentiality safeguarding confidential information while allowing publication of non-confidential information to fulfil project dissemination goals.

2.3 Summary

KEY ELEMENT OF THE IMPACT SECTION

SPECIFIC NEEDS	EXPECTED RESULTS	D & E & C MEASURES
What are the specific needs that triggered this project?	*What do you expect to generate by the end of the project?*	*What dissemination, exploitation and communication measures will you apply to the results?*
Need for Enhanced Privacy: Addressing concerns over personal data exploitation and lack of privacy in current digital interactions. **User-Controlled Data Sharing**: Empowering individuals to have control over how and with whom their data is shared. **Alternative to Surveillance-based Models**: Providing a platform that allows interaction with brands without the typical surveillance and data mining practices. **Building Trust in Digital Economy**: Establishing a trustworthy environment where users feel safe to share their data, knowing it will be used ethically and transparently.	**A Zero-Knowledge Advertising Protocol-Based Platform**: A groundbreaking platform that uses zero-knowledge advertising as an alternative to third-party cookies. **Effective Data Management Tools**: Enabling individuals to create, manage, and share their data efficiently with global organisations. **Value Exchange Mechanism**: A system where users can exchange their data for value, transforming how personal data is utilised. **Empowerment of EU Citizens**: Providing European citizens with a new, privacy-centric digital experience across the internet, enhancing their control and autonomy in the digital sphere.	**Brand Partnerships for Dissemination:** Collaborating with prominent brands to disseminate the platform's benefits, leveraging their reach to educate their customer base. **Communication Through Educational Institutions and Agencies**: Utilising academic channels and marketing agencies to communicate the platform's value and operational mechanism. **Targeted B2B Messaging:** Crafting messages tailored for business partners, highlighting the platform as a viable alternative to traditional advertising models. **Direct-to-Consumer Outreach:** Engaging directly with consumers to inform them about how they can take control of their data and derive better value from their internet experience.

TARGET GROUPS	OUTCOMES	IMPACTS
Who will use or further up-take the results of the project? Who will benefit from the results of the project?	*What change do you expect to see after successful dissemination and exploitation of project results to the target group(s)?*	*What are the expected wider scientific, economic, and societal effects of the project contributing to the expected impacts outlined in the respective destination in the work programme?*
Brands: Businesses will benefit from a new, ethical way to engage with consumers, enhancing brand loyalty and consumer trust. **Marketing Agencies:** Agencies can adopt this model for more effective and privacy-compliant advertising strategies. **Consumers**: Individuals gain more control over their data, leading to a more personalised and valuable digital experience. **Digital Economy:** Overall, the digital economy will benefit from a model that respects privacy while fostering innovation and economic growth.	**Enhanced Brand Experience:** Brands will experience a more private and exclusive interaction with consumers, leading to deeper engagement. **Improved Marketing Outcomes:** Marketing strategies will yield better results due to more targeted and consent-based consumer interactions. **Greater Value for All Parties:** Both brands and consumers will benefit from fairer value exchange, enhancing satisfaction on both ends. **Elimination of Surveillance:** The shift to a privacy-focused model will eliminate the need for intrusive surveillance tactics in marketing.	**Scientific Breakthrough:** Establishing a new internet protocol that revolutionises commercial interactions online, significantly advancing the current state of internet technology. **Economic Efficiency:** Drastically reducing advertising fraud, potentially saving between 40-70% of advertising budgets currently lost to fraudulent activities. **Enhanced Quality of Advertising:** Achieving a higher quality in advertising through precise and fraud-free methods. **Societal Benefit:** Offering a more enjoyable and private internet experience, free from the intrusive practices of surveillance-based advertising.

#§IMP-ACT-IA§#

3. Quality and efficiency of the implementation #@QUA-LIT-QL@# #@WRK-PLA-WP@#

3.1 Work plan and resources

Our approach to the work plans has been meticulously designed to converge on a singular, pivotal milestone that unifies the efforts of all work packages into a comprehensive solution. By strategically sequencing tasks, from technical program management to backend development, we ensure that each phase not only contributes to its specific domain but also integrates seamlessly into the larger project framework. This cumulative methodology allows for a structured yet flexible progression, with each work plan layering upon the previous one, culminating in a robust and innovative solution that meets the Horizon 2020 project's ambitious goals.

For Horizon 2020 projects, the methodology is entrenched in a collaborative and iterative process, ensuring cross-disciplinary input and ongoing validation against project objectives. The foundation of our work plan methodology is built upon clear, measurable, and attainable milestones, with integrated checkpoints for quality assurance, risk assessment, and compliance verification. Regular reviews and adaptive planning are embedded to align with evolving project landscapes and stakeholder feedback. This dynamic approach guarantees that as we reach the delivery of each key milestone, we are not only achieving individual work package goals but also advancing towards the realisation of the overarching solution, reflective of the collaborative ethos and innovative spirit of the Horizon 2020 initiative.

Work plan structure, risks, and mitigations

A New Internet Experience – WP1

Work Plan:

This work plan has been methodically crafted to enhance our tool, with ongoing improvements based on user feedback. The plan includes rigorous testing and iterative updates, ensuring the tool's functionality meets evolving needs.

- **Tasks Assignment**: We will incorporate headline design tasks such as UI/UX enhancements, feature updates, and system optimisation.
- **Budget Justification**: The budget is meticulously justified, aligning person-months with detailed task requirements, ensuring each monetary allocation directly contributes to specific project objectives.
- **Partner Profiles**: Each partner's expertise is strategically matched to their tasks, ensuring their capacity and skills are optimally utilised.
- **Collaborative Value**: Collaboration is structured to leverage the unique strengths of each partner, fostering innovation and efficiency.

Risks and Mitigations:

- **Risk**: Potential delays in design implementation. Mitigation involves allocating additional person-months to ensure timely delivery, with Profila dedicating 30 person-months to design creation, testing, and improvement to pre-emptively address this risk.

A Profila: A Privacy-Preserving Profile for a New Internet – WP2

Work Plan:

This work plan has been meticulously structured, focusing on the continuous enhancement of our platform through user-centric design and feedback-driven iterations. It includes:

- **Tasks Assignment**: The development of Digital Identities using DIDs, establishment of Data Spaces based on the Solid Flanders Pod, and the implementation of Multi-party Computation and a blockchain ledger system. These tasks ensure secure, verified data sharing and privacy-preserving insights.
- **Budget Justification**: Resources are allocated to fulfil these tasks, with budgetary provisions reflecting the

person-months and expertise required for each component.

- **Partner Profiles**: Profila, Partisia and Parhelium bring specialised skills to the project, ensuring technical and design tasks are executed with precision.

Collaborative Value: This project is a synergy of efforts, combining advanced technology implementation with strategic partner collaboration to enhance digital privacy and identity management.

Risks and Mitigations:

- **Risk**: Potential delays in technology implementation and integration due to complexities of MPC in distributed data storage. Mitigation involves allocating additional person-months to ensure timely research into the challenge is conducted.

A Zero Knowledge Advertising Protocol: The Cookie Killer – WP3

Work Plan:

This work plan is comprehensive, addressing the development and integration of key components such as digital identities, privacy-preserving computation and a blockchain-based audit trail. Partnering with industry leaders, we're tackling the challenges of secure digital identities and high-volume data analytics. We're working on creating digital IDs that mesh with the European eID framework, enhancing the platform's utility and trustworthiness. For computation, we're collaborating with Partisia, leveraging their expertise in multiparty computation to ensure data security on a large scale.

1. **Integration of Digital Identities**: Collaborating with key EU digital identity frameworks to integrate decentralised identifiers.
2. **Development of Data Spaces**: Constructing secure and private data spaces based on open-source principles.
3. **Deployment of Multi-party Computation**: Establishing advanced computation techniques for data analysis without compromising privacy.
4. **Implementation of Blockchain Ledger**: Recording identity verifications and transactions to ensure transparency and user control.

Risks and Mitigations:

- **Risk of Adoption**: There may be resistance to transitioning away from third-party cookies. We plan to mitigate this by engaging with stakeholders early and demonstrating clear benefits.
- **Technical Integration Challenges**: The integration of new technologies may present unforeseen technical hurdles. We will allocate additional resources and expertise to address potential integration issues promptly.
- **Regulatory Compliance**: As regulations evolve, there may be risks of non-compliance. Our mitigation strategy includes ongoing monitoring of regulatory changes and proactive adaptation of our technology.

A Better Data and Attention Business Model – WP4

Work Plan:

Our work plan involves a multi-phase approach to creating a sustainable business model. Initially, we will focus on in-depth market research to understand how users value their data and attention. Following this, we will develop prototypes that align monetary incentives with user engagement, without compromising privacy. These prototypes will be iteratively refined based on user feedback and legal consultation to ensure GDPR compliance.

Risks and Mitigations:

- **Privacy Breach Risk**: Implementing rigorous data protection protocols to mitigate this risk.

- **User Manipulation Risk**: Ensuring transparency in how data and attention are monetised to avoid manipulation.
- **Legal and Compliance Risk**: Continuous monitoring of regulatory changes to adapt our model accordingly.
- **Market Acceptance Risk**: Engaging with potential users and stakeholders early to validate our model and adapt to market demands.

A Privacy by Design Platform – WP5

Work Plan:

The work plan is designed to be comprehensive and iterative, involving a continuous cycle of assessment, adjustment and enhancement. It encompasses:

- Regularly conducting Privacy Impact Assessments (PIAs) to proactively spot and evaluate privacy risks.
- Transparently documenting data processing activities, reinforcing our commitment to openness.
- Employing detailed data mapping to maintain an accurate inventory of personal data, supporting the principle of data minimisation and ensuring clarity of purpose for data usage.

Risks and Mitigations:

- **Privacy Regulation Compliance Risk**: The potential for non-compliance with evolving privacy regulations. Mitigation will involve regular legal reviews and updates to our practices.
- **Data Breach Risk**: The possibility of unauthorised access to personal data. Mitigation measures include robust cybersecurity protocols and regular system audits.
- **Technology Implementation Risk**: Challenges in integrating new privacy technologies. Mitigation will be addressed by phased testing and deployment, ensuring compatibility and functionality before full-scale implementation.

A Sandbox for Enterprise to Learn – WP6

Work Plan:

The work plan encompasses a coordinated effort across various interactive and analytical fronts to advance market reach. Activities include regular events, forums and summits designed to engage a community of experts. A specialised tool will be crafted for deep technological dives, alongside another tool dedicated to risk and opportunity assessment. A dedicated environment will support the creation and testing of new concepts, aligning closely with the innovation and decision-making processes within the corporate sector. Risk management will involve proactive strategies and iterative feedback incorporation to maintain the relevance and efficacy of the digital identity and privacy initiatives.

Risks and Mitigations:

- **Engagement Risk**: There's a possibility that the planned events may not fully engage the target expert community.
- **Technological Adaptation Risk**: The specialised tools developed may face challenges in user adoption or may not meet all analytical needs.
- **Innovation Implementation Risk**: New concepts and prototypes may not align with existing market needs or corporate decision-making processes.
- **Feedback Integration Risk**: There is a risk that feedback may not be adequately captured or integrated, potentially leading to misalignment with project goals.

Mitigation strategies for these risks will involve dynamic engagement tactics, iterative user testing of tools, flexible concept development responsive to market feedback and robust mechanisms for capturing and acting on stakeholder input.

Project coordination and management – WP7

Work Plan:

The core objectives of WP7 in managing this project are as follows:

- Establishing and maintaining a decision-making process to ensure effective coordination.
- Setting up a robust system for the seamless flow of both technical and organisational information among all project participants.
- Implementing continuous monitoring of the project's progress and budget, keeping track of any developments or deviations and reporting these both within the consortium and to the European Commission.
- Providing diligent administrative management to meet all contractual obligations and facilitating constructive communication among consortium members, the European Commission and external collaborators.
- Overseeing the entire project to ensure compliance with legal and data management standards.

Project Management: The task involves overseeing both technical and administrative aspects to ensure efficient and timely execution of project work. This includes monitoring activities, managing financial and administrative resources and preparing regular project reports. Periodic reports, including financial and technical details, will be submitted to the European Commission annually.

Technical Management: Led by the designated leader, this task focuses on monitoring project progress, particularly in achieving technical and scientific goals. It involves quality assurance and risk management to detect and correct errors and deviations early in the project life cycle.

Legal and Data Management: This task manages legal and ethical aspects of the project, including data protection, intellectual property and contractual aspects. It involves providing legal guidance for all deliverables and supervising data management, ensuring compliance with open data obligations. A Data Management Plan will be created and updated throughout the project.

To effectively manage all teams and deliverables in our project, we will utilise EMDESK online project management software. EMDESK offers a comprehensive approach to managing Horizon Europe projects, focusing on efficiency and collaboration. Here are some aspects of EMDESK's methodology that we will incorporate into our project management:

1. **Comprehensive Project Management**: EMDESK enables management of the entire project lifecycle, from planning and financial management to reporting and collaboration.
2. **Real-Time Project Visibility**: It allows for maintaining real-time visibility of project progress, finances and deadlines, ensuring all activities, milestones and deliverables are tracked accurately.
3. **Efficient Collaboration Tools**: The software supports secure collaboration and sharing of documents and reports, streamlining communication with tools like messaging, reminders and video conferencing.
4. **Time-Saving Features**: EMDESK simplifies tasks such as proposal creation and reporting, potentially saving up to 30% of consortium time and provides a central hub for hassle-free reporting and data management.
5. **User-Friendly Setup and Support**: EMDESK offers services such as direct data import, project setup and coordinator and partner onboarding sessions, backed by a help desk with video tutorials. Their team,

experienced in Horizon Europe project management, offers fast, dedicated support to ensure smooth operation.

By integrating EMDESK's methodology, we aim to enhance the efficiency and effectiveness of our project management, ensuring that all teams and deliverables are optimally coordinated and communicated.

Project Timing – Gantt Chart

WP1	A New Experience	Contributor	Resource	Person Months	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30
WP1.1	Technical program and product management	Profila	Technical Programe Director	12																														
WP1.2	Design and R&D management	Profila	Design & R&D Manager	12																														
WP1.3	Design lifecycle management	Profila	Designer - SNR	30																														
WP1.4	Design implementation and testing	Profila	Designer & CX Expert	30																														
WP1.5	Frontend platform development	Parhelium	Fronted Developer	30																														
WP1.6	Frontend platform development	Parhelium	Fronted Developer - SNR	12																														
WP1.7	Logic & integration development	Parhelium	Integration Developer	12																														
WP1.8	Backend development	Parhelium	Backend Developer	12																														
WP2	A Profila																																	
WP2.1	Technical program and product management	Profila	Technical Programe Director	6																														
WP2.2	Design and R&D management	Profila	Design & R&D Manager	8																														
WP2.3	Web3 Digital ID implementation	Partisia	Partisia Developer1	18																														
WP2.4	Web3 optimisation & integration	Parhelium	Web3 Developer	24																														
WP2.5	Data spaces implementation	Parhelium	Integration Developer	4																														
WP2.6	Web3 Encryption, MPC analytics, ledger	Partisia	Partisia Developer2	18																														
WP2.7	Logic & integration development	Parhelium	Integration Developer	4																														
WP2.8	Backend development	Parhelium	Backend Developer	8																														
WP3	A Zero Knowledge Advertising Protocol																																	
WP3.1	Technical program and product management	Profila	Technical Programe Director	3																														
WP3.2	Design and R&D management	Profila	Design & R&D Manager	5																														
WP3.3	Protocol design and implementation	UC3M	Researcher Dev	30																														
WP3.3	Protocol design and implementation	UC3M	Researcher Dev	30																														
WP3.3	Protocol design and implementation	UC3M	Researcher Dev	30																														
WP3.4	Web3 optimisation & integration	Parhelium	Web3 Developer	6																														
WP3.5	Logic & integration development	Parhelium	Integration Developer	10																														
WP3.6	Backend development	Parhelium	Backend Developer	10																														
WP3.7	Web3 integrations, DID, data spaces	Partisia	Partisia Developer1	12																														
WP3.7	Web3 integrations, encryption, MPC, ledger	Partisia	Partisia Developer2	12																														
WP4	A Better Data & Attention Business Model																																	
WP4.1	Technical program and product management	Profila	Technical Programe Director	3																														
WP4.2	Design and R&D management	Profila	Design & R&D Manager	3																														
WP4.3	Research, surveys, documentation	Profila	SNR Consultant	12																														
WP4.4	Model creation and testing	Profila	JNR Consultant	8																														
WP5	A Privacy by Design Platform																																	
WP5.1	Technical program and product management	Profila	Technical Programe Director	3																														
WP5.2	Design and R&D management	Profila	Design & R&D Manager	2																														
WP5.3	Legal management	DeRoos	Lawyer SNR	6																														
WP5.4	Compliance assessments	DeRoos	Lawyer JNR1	3																														
WP5.4	Compliance assessments	DeRoos	Lawyer JNR2	3																														
WP6	A Sandbox for enterprise																																	
WP6.1	Technical program and product management	Profila	Technical Programe Director	3																														
WP6.2	Sandbox design	Profila	SNR Consultant	10																														
WP6.3	Sandbox implementation and trials	Profila	JNR Consultant	20																														
WP6.4	Industry performance and integration	Publicis	Senior Performance Specialist	30																														
WP6.5	ISO readiness	Profila	SNR Consultant	18																														
WP7	Project management																																	
WP7.1	Horizon programme management	DeRoos	Horizon Project Director	30																														
WP7.2	Technical delivery project management	Profila	Project Manager - technical	30																														
WP7.3	Legal project delivery	DeRoos	Project manager - legal	6																														

3.2 Capacity of participants and consortium as a whole #@CON-SOR-CS@# #@PRJ-MGT-PM@#

Consortium Leadership and Legal Expertise: De Roos Legal, leading the consortium, ensures a stringent adherence to privacy regulations. Their expertise in legal compliance and privacy law is pivotal in navigating the complex legal landscape of digital platforms. Their presence makes the consortium robust in both technology and legal acumen. The law firm exists for 10 years, counts 50 lawyers and has an experience managing large scale projects.

Platform Development and Strategic Contributions: Profila Switzerland now spearheads platform development, excelling in product management and user centric UX and UI design, ensuring a seamless user experience and efficient project execution. Their expertise extends to solution architecture, creating robust, adaptable platform architectures that align with both technical needs and strategic objectives. Profila's role also includes business model research, focusing on developing sustainable, scalable models and ensuring the platform's long-term viability.

Enterprise Sandbox Development and Compliance: A key outcome of their business model research is the development of an enterprise sandbox. This environment allows enterprises to test and explore the platform's features safely, demonstrating its utility and integration potential in real-world business scenarios. Additionally, Profila Switzerland is responsible for ensuring ISO compliance, adhering to international standards in quality management, data security and privacy, thus ensuring the platform's high standards of quality and reliability, crucial for user trust and legal compliance.

Advanced Technical Development and Integration: Parhelium in Poland specialises in the technical development and integration of the platform. Their technical prowess in software engineering and system integration is critical for building a robust and scalable platform.

Cutting-edge Research and Protocol Implementation: The University Carlos III of Madrid contributes significantly with their cutting-edge research capabilities, particularly in the implementation of the zero-knowledge advertising protocol. This ensures a balance between advertising efficacy and user privacy.

Data Analytics and Multi-Party Computation: Partisia in Denmark implements multi-party computation for data analytics. Their expertise in advanced computation methods enhances the platform's ability to process data securely and efficiently, contributing significantly to data-driven decision-making processes.

Advertising Performance Analysis and Customer Engagement: Digitas (Publicis Bulgaria) joins the consortium to focus on analysing the platform's advertising performance. Their role in assessing the effectiveness of advertising strategies with agencies and brand customers is crucial. They also ensure the implementation of a customer feedback loop, providing vital insights for continuous improvement.

Access to Critical Infrastructure: De Roos Legal offers academic and legal research facilities, while Profila Switzerland brings in its product management and design expertise. Parhelium contributes with technical development infrastructure and the University Carlos III of Madrid provides advanced research facilities. Partisia and Digitas add their specialised computational and analytical capabilities, respectively.

Complementarity and Value Chain Coverage: Each member complements the others effectively. De Roos Legal ensures legal compliance, Profila Switzerland leads in product management and design, Parhelium brings technical development expertise and the University Carlos III Madrid adds protocol implementation research. Partisia enhances the data analytics aspect, while Digitas focuses on advertising performance and customer engagement.

Industrial/Commercial Involvement: Profila Switzerland, along with Parhelium, ensures the commercial exploitation of the project. Digitas' role in analysing advertising effectiveness and customer feedback is pivotal in aligning the project with market needs and exploitation strategies.

International Participation: Participants from eligible EU funding countries ensure seamless collaboration and funding allocation. The consortium's diverse geographic distribution enhances the project's impact across the EU, leveraging each member's unique strengths.

#§CON-SOR-CS§# #§PRJ-MGT-PM§#

Tables for section 3.1

Table 3.1a: List of work packages

Work package No	Work Package Title	Lead Participant No	Lead Participant Short Name	Person-Months	Start Month	End month
WP1	A New Experience	4	Profila	150	Month1	Month30
WP2	A Profila	4	Profila	90	Month1	Month30
WP3	A Zero Knowledge Advertising Protocol	2	UC3M	148	Month1	Month30

WP4	A Better Data and Attention Business Model	4	Profila	26	Month1	Month30
WP5	A Privacy by Design Platform	1	De Roos	29	Month1	Month30
WP6	A Sandbox for enterprise	4	Profila	81	Month1	Month30
WP7	Project management	1	De Roos	66	Month1	Month30

Table 3.1b: Work package description

For each work package:

Work package number	1
Work package title	A new experience

Objectives

The overarching objective is to develop a transformative user experience (UX) and user interface (UI) for the platform, which is essential not only to its functionality but also to fostering new user behaviours. This will empower users to take control of their data and derive value from exchanging it with organisations. The work plan includes managing the entire design lifecycle, from technical program oversight to research and development (R&D) management, ensuring each phase—conceptualisation, implementation and testing—meets our high standards for innovation and practicality. By focusing on a user-centric design approach and integrating robust frontend and backend development processes, we aim to create an intuitive and seamless interface that encourages user engagement and trust, ultimately leading to a widespread adoption of new data-sharing practices.

Description of work

1. **Technical Program and Product Management**: Establish a framework for overseeing the project's technical aspects and product lifecycle, ensuring that all technical deliverables align with the strategic objectives.
2. **Design and R&D Management**: Develop a research and design strategy that promotes innovation and practical application, while managing resources and timelines for R&D activities.
3. **Design Lifecycle Management**: Implement a comprehensive approach to manage the entire design process, from conceptualisation to final product delivery, ensuring consistency and quality at each stage.
4. **Design Implementation and Testing**: Apply rigorous testing protocols to validate design implementations, ensuring that they meet the required specifications and user expectations.
5. **Frontend Platform Development**: Build a user-centric and responsive frontend platform that delivers a seamless experience across different devices and platforms.
6. **Logic and Integration Development**: Create robust backend logic that supports platform functionality and integrates seamlessly with frontend components and third-party systems.
7. **Backend Development**: Construct a scalable and secure backend infrastructure that underpins the platform's operations, ensuring data integrity and system reliability.

Work package number	2
Work package title	A Profila (A personal Profile)

Objectives

The principal objective of this work plan is to forge 'Profila', a singular, consolidated profile platform that empowers every individual to create, maintain, share and monetise their digital identity and data across the internet. We aim to intertwine advanced Web3 technology, including Digital ID implementation and MPC data analytics, with robust backend development and strategic R&D management. This endeavour will streamline user experiences, optimise data transactions for value creation and foster seamless integration within the digital economy. Through meticulous program management and a focus on user-centric design, 'Profila' will set a new benchmark for personal data agency and economic participation on the web.

Description of work

1. **Technical Program and Product Management**: Oversee the product's lifecycle and technical roadmap, ensuring that development milestones are aligned with strategic goals and market expectations.
2. **Design and R&D Management**: Manage and coordinate the design and research efforts, focusing on innovative features that enhance user experience and platform functionality.
3. **Web3 Digital ID Implementation**: Implement a secure and user-centric digital identity solution using Web3 technologies, facilitating a new standard of user authentication and ownership.
4. **Web3 Optimisation and Integration**: Optimise the platform's Web3 integration to ensure smooth, decentralised operations and user interactions within the blockchain ecosystem.
5. **Data Spaces Implementation**: Develop dedicated data spaces that allow for secure data exchange, ensuring privacy and compliance with regulatory standards.
6. **Web3 Encryption, MPC Data Analytics, Activity Ledger**: Incorporate advanced encryption and multi-party computation (MPC) for data analytics, along with a transparent activity ledger for enhanced security and user trust.
7. **Logic and Integration Development**: Build and refine the platform's logic and integration layers to support seamless functionality and interoperability with external systems.
8. **Backend Development**: Establish a robust backend infrastructure that ensures the platform's scalability, reliability and performance.

Work package number	3
Work package title	A Zero Knowledge Advertising Protocol

Objectives

The objective of this work plan is to develop a pioneering Zero Knowledge Advertising Protocol that will revolutionise online privacy, marking the end of third-party cookie tracking. Our focused efforts in technical program management, sophisticated design and R&D will pave the way for the creation of a protocol that enables private, surveillance-free internet experiences. By integrating state-of-the-art Web3 technologies, encryption and multi-party computation, we will construct a system where advertisements are targeted effectively without compromising user anonymity. This protocol will be the cornerstone of a new era in digital advertising—where user consent and data sovereignty are paramount and the invasive practices of the past are rendered obsolete.

Description of work

1. **Technical Program and Product Management**: Direct the program's progression, ensuring that the development of the Zero Knowledge Advertising Protocol adheres to project timelines and quality benchmarks.
2. **Design and R&D Management**: Lead the design research, focusing on the creation of a privacy-centric advertising protocol that aligns with cutting-edge R&D insights.
3. **Protocol Design and Implementation**: Craft and execute the Zero Knowledge Protocol, aiming for minimal data exposure while maintaining the efficacy of digital advertising.
4. **Web3 Optimisation and Integration**: Enhance the advertising protocol's performance and user interaction through the strategic integration of Web3 technologies.
5. **Logic and Integration Development**: Construct logical frameworks and integration pathways that support the seamless functionality of the advertising protocol within the platform's broader ecosystem.
6. **Backend Development**: Develop a secure and scalable backend system that supports the complex demands of the Zero Knowledge Advertising Protocol.
7. **Web3 Integrations, DID, Data Spaces**: Implement decentralised identity (DID) and dedicated data spaces to facilitate a secure and user-controlled advertising environment.
8. **Web3 Integrations, Encryption, MPC, Ledger**: Incorporate advanced encryption methods, multi-party computation (MPC) and a comprehensive activity ledger to ensure the integrity and transparency of advertising operations.

Work package number	4
Work package title	A Better Data and Attention Business Model

Objectives

The core objective of this work plan is to establish a groundbreaking business model focused on the monetisation of personal data and user attention. This model will be developed through a blend of market analysis and scientific research, ensuring a deep understanding of user behaviours and preferences. We will engage in a meticulous process of technical program management, design and R&D management, along with extensive research, surveys and documentation. The aim is to create and test a model that ethically balances user engagement with data integrity, reshaping the way personal data and user attention are valued and utilised in the digital economy. This initiative will not only enhance user empowerment in data transactions but also set new standards for responsible and sustainable monetisation practices in the digital world.

Description of work

1. **Technical Program and Product Management**: Coordinate the development of the 'A Better Data and Attention Business Model' initiative, ensuring that all technical aspects and product developments are strategically aligned with the model's objectives.
2. **Design and R&D Management**: Lead the design and research activities, focusing on the creation of innovative business models that prioritise user attention and data integrity.
3. **Research, Surveys, Documentation**: Conduct comprehensive research and surveys to gather insights into user behaviour and preferences and meticulously document findings to inform the development of the business model.
4. **Model Creation and Testing**: Develop and rigorously test a new business model that leverages these insights, aiming to balance user engagement with ethical data practices, ultimately transforming how user attention and data are valued and monetised in the digital landscape.

Work package number	5
Work package title	A Privacy by Design Platform

Objectives

The primary objective of this initiative is to rigorously develop and implement comprehensive privacy impact assessments and data mappings as integral parts of our 'A Privacy by Design Platform'. This approach is aimed at ensuring the platform empowers individuals with unparalleled control over their data and privacy during online interactions. Through rigorous technical program management, informed design and R&D management and stringent legal and compliance assessments, we intend to establish a platform that not only meets but exceeds current privacy standards. By embedding privacy into the very fabric of the platform, we aspire to create a digital environment where user trust is paramount and data sovereignty is a reality for every user.

Description of work

1. **Technical Program and Product Management**: Oversee the development of the 'A Privacy by Design Platform', ensuring that all technical elements are meticulously aligned with privacy-first principles throughout the platform's lifecycle.
2. **Design and R&D Management**: Direct the research and design process, focusing on integrating privacy by design concepts into every aspect of the platform, from initial sketches to final implementation.
3. **Legal Management**: Collaborate with legal experts to incorporate privacy laws and regulations into the platform's structure, ensuring that all design and development activities comply with legal standards.
4. **Compliance Assessments (First Phase)**: Conduct initial compliance assessments to evaluate the platform's adherence to privacy regulations and standards, identifying areas for improvement or modification.
5. **Compliance Assessments (Ongoing)**: Implement a continuous compliance assessment process to regularly review and update the platform, ensuring sustained alignment with evolving privacy laws and user expectations.

Work package number	6
Work package title	A Sandbox for enterprise

Objectives

The overarching goal of this work plan is to create an advanced 'Sandbox for Enterprise', a dedicated environment where businesses can trial our platform, enabling them to fully understand its innovative approach to data and privacy management. This sandbox will be meticulously designed, implemented and tested to ensure it meets enterprises' needs. The design will emphasise adaptability, security and will comply with international standards such as those provided by the ISO. Crucially, industry representative Digitas will play a key role by engaging directly with enterprises to test the platform, gather feedback and provide critical insights into ways the platform may be improved. These interactions are intended not only to refine the platform's performance but also to demonstrate the tangible benefits of our data and privacy solutions, thereby facilitating a smoother adoption process. Ultimately, this sandbox aims to be a catalyst for enterprises to experience first-hand the transformative impact of our platform, fostering trust and driving widespread acceptance in the business community.

Description of work

1. **Technical Program and Product Management**: Lead the overall direction and coordination of the 'A Sandbox for Enterprise' project, ensuring all technical developments align with enterprise needs and project objectives.
2. **Sandbox Design**: Design a versatile and secure sandbox environment tailored for enterprises, focusing on adaptability and scalability to accommodate various industry requirements.
3. **Sandbox Implementation and Trials**: Implement the sandbox with robust functionalities, conducting comprehensive trials to validate its effectiveness and efficiency in a controlled setting.
4. **Industry Performance and Integration**: Evaluate and enhance the sandbox's performance and integration capabilities with existing enterprise systems, ensuring seamless functionality and user experience.
5. **ISO Readiness**: Prepare the platform for ISO compliance, ensuring adherence to international standards in quality management and security, thereby reinforcing its reliability and trustworthiness for enterprise use.

Work package number	7
Work package title	Project management

Objectives

The fundamental objective of this work package is to meticulously implement project management best practices, ensuring the delivery of a project that not only aligns with but also exemplifies the high standards set by the Horizon 2020 programme. Our approach encompasses comprehensive management of all project facets, from rigorous technical delivery and legal compliance to effective programme administration. By integrating these elements seamlessly, we aim to foster a robust and collaborative environment that is conducive to achieving our ambitious project goals. The emphasis will be on maintaining strict adherence to Horizon 2020 guidelines, utilising cutting-edge methodologies and ensuring a cohesive and synergistic effort among all stakeholders. This approach will guarantee the project's success, setting a benchmark for excellence in the realm of EU-funded initiatives.

Description of work

1. **Project Management**: Oversee the entire Horizon 2020 project, coordinating all aspects from conceptualisation to execution, ensuring that project objectives are met efficiently and effectively.
2. **Horizon Programme Management**: Specifically manage the Horizon 2020 programme aspects, ensuring compliance with the programme's guidelines, timelines and objectives, and facilitating smooth collaboration among all stakeholders.
3. **Technical Delivery Project Management**: Lead the technical aspects of the project, managing the development and implementation of technological solutions, while ensuring they align with the project's goals and comply with technical standards.
4. **Legal Project Delivery**: Handle all legal aspects of the project, including compliance with EU regulations and guidelines, managing contractual obligations and ensuring all activities adhere to legal requirements within the Horizon 2020 framework.

Table 3.1c: List of Deliverables

Number	Deliverable name	Short description	Work package number	Short name of lead participant	Type	Dissemination level	Delivery date (in months)
1	Project Plan	Project Plan	1,2,3,4,5,6,7	Profila	R	PU	3
2	Design Plan	Designs and Methodology	1	Profila	R, DEM	PU	6
3	Solution Architecture	Solution Architecture Document (Incl. Data Management Plan)	1	Profila	R, DMP	PU	6
4	Platform UI	Platform UI (WebApp)	1	Profila	Other	PU	18
5	Web3 Architecture	Web 3 Solution Architecture Document	2	Profila	R	PU	3
6	Data Space Architecture	POD Data Space Solution Architecture Document	2	Profila	R,	PU	3
7	MPC Architecture	MPC Architecture Document	2	Profila	R	PU	6
8	Web3 Profila (Profile)	Web3 Profile with Distributed Storage (WebApp)	2	Profila	Other, DATA	PU	30
9	MPC Architecture	MPC Architecture Document	2	Profila	R	PU	6
10	Zero Knowledge Protocol Architecture	ZKA Architecture Document	3	UC3M	R	PU	6
11	ZKA and MPC Integration Architecture	ZKA and MPC Architecture Document	3	UC3M	R	PU	6
12	A ZKA Protocol	A ZKA Protocol integrated with MPC and Delivering from a RTB Ad Server	3	UC3M	Other, DEM	PU	30
13	Data and Attention Business Model Theory and Research	Business Model Theory and Research Document	4	Profila	R	PU	12
14	Data and Attention Business Model Tool	Data and Attention Business Model Tool	4	Profila	Other	PU	12
15	Privacy by Design	Privacy by Design Strategy Document	5	De Roos	R	PU	3

	Strategy						
16	Privacy Audits	DPIA and Data Mapping Audit	5	De Roos	R	PU	24
17	Regulatory Compliance Assessment	Regulatory Compliance Assessment Document	5	De Roos	R	PU	24
18	Enterprise Sandbox Strategy	Enterprise Sandbox Strategy Document	6	Profila	R	PU	3
19	Sandbox design, processes and methodology	Sandbox design, processes and methodology document	6	Profila	R	PU	6
20	Enterprise and agency market fit	Enterprise and agency market fit strategy document	6	Profila	R	PU	6
21	Enterprise Sandbox	An Enterprise Sandbox	6	Profila	Other	PU	24
22	Enterprise market fit report	Enterprise market fit report	6	Profila	R	PU	30
23	ISO readiness	An ISO Readiness assessment incl. Required Documentation for audit	6	Profila	R	PU	24

Table 3.1d: List of milestones

Milestone number	Milestone name	Related work package(s)	Due date (in month)	Means of verification
1	Platform UI	1	18	Demonstration
2	A Web3 Profile with Distributed Storage	2	30	Demonstration
3	A ZKA Protocol integrated with MPC and Delivering from a RTB Ad Server	3	30	Demonstration
4	Data and Attention Business Model Tool	4	12	Demonstration
5	Regulatory Compliance Assessment Document	5	24	Documentation Presentation
6	An Enterprise Sandbox	6	30	Demonstration and Documentation

Table 3.1e: Critical risks for implementation #@RSK-MGT-RM@#

Description of risk (indicate level of (i) likelihood and (ii) severity: Low/Medium/High)	Work package(s) involved	Proposed risk-mitigation measures
WP1 - delays in design implementation - Medium	1	Design methodology planning and implementation
WP2 - Potential delays in technology implementation and integration due to complexities of MPC in distributed data storage. Mitigation involves allocating additional person-months to ensure timely research into the challenge is conducted - Medium	2	Research into advanced MPC capabilities by world leading MPC team.
WP3 - Technical Integration Challenges: The integration of new technologies in the ZKA protocol may present previously unforeseen technical hurdles.	3	Research into AdTech methods and capabilities by experienced AdTech research team.
WP4 - Market Acceptance Risk - Medium	4	Engaging with potential users and stakeholders early to validate our model and adapt to market demands with the aid of our industry partner Digitas/Publicis
WP5 - Data Breach Risk: The possibility of unauthorised access to personal data. - Medium	5	Mitigation measures include robust cybersecurity protocols and regular system audits.
WP6 - Feedback Integration Risk: There is a risk that feedback may not be adequately captured or integrated, potentially leading to misalignment with project goals.	6	Mitigated with the aid of our industry partner Digitas/Publicis who have multiple brand relationships.

#§RSK-MGT-RM§#

Table 3.1f: Summary of staff effort

	WPn	WPn+1	WPn+2	Total Person-Months per Participant
1. De Roos	5+12	6+36		48
2. UC3M	3+90			90
3. Partisia	2+36	3+24		60
4. Profila	1+84	2+14	3+8, ç+26, 5+5, 6+81, 7+30	218
5. Publicis Bulgaria	6+30			30
6. Parhelium sp zoo	1+66	2+40	3+26	132
Total Person Months				578

Table 3.1g: 'Subcontracting costs' items

Participant Number/Short Name		
	Cost (€)	**Description of tasks and justification**
Subcontracting		

Table 3.1h: 'Purchase costs' items (travel and subsistence, equipment and other goods, works and services)

Participant Number/Short Name		
	Cost (€)	**Justification**
Travel and subsistence	182.220	Quarterly principal team meetings – all in EU and ad-hoc program management 1:1 meeting. Meetings with Enterprise customers in the trials.
Equipment	546,660	Equipment for the team, standard issue laptops and infrastructure and licencing for hosting the relevant platform components.
Other goods, works and services	409,995	Contingency budget for further project delivery requirements.
Remaining purchase costs (<15% of pers. Costs)		
Total	1,138,875	

Table 3.1i: 'Other costs categories' items (e.g., internally invoiced goods and services)

Participant Number/Short Name		
	Cost (€)	**Justification**
Internally invoiced goods and services		
…		

Table 3.1j: 'In-kind contributions' provided by third parties.

Participant Number/Short Name			
Third party name	**Category**	**Cost (€)**	**Justification**
	Select between Seconded personnel Travel and subsistence Equipment Other goods, works and services Internally invoiced goods and services		

Annex 1 – Zero Knowledge Advertising research paper

Zero Knowledge Advertising: a new era of privacy-preserving AdTech solutions

Patricia Callejo*, Rubén Cuevas*†, Ángel Cuevas*† Mikko Kotila‡, Luke Bragg‡, Michiel Van Roey‡
*UC3M-Santander Big Data Institute, Spain
† Universidad Carlos III de Madrid, Spain
‡ Profila GmbH, Switzerland

***Abstract*—The new data protection legislation along with the social pressure has encouraged the online advertising industry to propose novel privacy-preserving advertising solutions, such as Brave or Google's FLoC. While these pioneering solutions represent an undoubtedly important step towards a more ethical form of targeted advertising, they present some limitations. In this paper, we first systematically identify the limitations of the most promising industrial solutions. Armed with such knowledge, we present a new (simple and efficient) privacy preserving solution for delivering targeted ads, which combines the benefits of state-of-the-art proposals. To confirm the operational viability of our solution in the current online advertising ecosystem, we have performed extensive simulation experiments assessing that: 1) our solution requires a minimal use of device's resources (memory and CPU), making it valid for handheld devices running on limited power batteries; 2) it meets the strict timing requirements for the delivery of ads imposed in the online advertising ecosystem.**

I. Introduction

Online advertising is superior to other forms of advertising (e.g., TV or newspapers) due to its capacity of delivering personalized ads. To exploit this advantage online advertising stakeholders have developed a sophisticated tracking ecosystem able to track the activity of users online, but also offline, leveraging the sensors and GPS information retrieved from connected smartphones. The questionable tracking practices used by some players in the online advertising ecosystem has led to numerous scandals related to the potential misuse of users' personal data [1], [2], [3]. Those continuous scandals have increased the social and legal pressure [4], [5] on Ad Tech companies urging them to change their business models towards more privacy-preserving and ethics-oriented solutions.

We can find few recent efforts by industry such as Brave browser [6], Google's Federated Learning of Cohorts (FLoC) [7], [8] or Personal Data Platforms (PDPs) [9], [10], [11], [12] that represent a clear step in the market towards (at least reasonably) privacy-preserving ad delivery solutions. While these pioneering solutions represent doubtlessly important contributions to the field, they still have some limitations. For instance, some of these solutions, such as the Brave browser, operate as walled gardens limiting their operation to specific venues. Other approaches, such as FLoC or PDPs, do not offer the possibility of running full-private advertising processes (a.k.a. zero knowledge advertising) or enable auditability.

In this paper, we present a novel and comprehensive solution that tries to overcome the limitations of the existing state-of-the-art proposals. We rely in two main principles, simplicity and efficiency, and leverage basic cryptography technologies to propose a first version of our solution. The main functionalities of our solution are: 1) It is actionable in different venues (e.g., mobile apps, web browsers, video platforms) contrary to walled garden approaches; 2) It offers two operation modes: (i) the default mode is zero knowledge advertising, where personalized ads are delivered to users without sharing any users' data with third parties. (ii) The second mode is referred to as *consent-based advertising*, and it requires the proactive action of the user to activate it. In this mode, the user explicitly selects what personal data items (if any) they are willing to share with each advertiser. To illustrate this mode, let us think of a scenario where a user is willing to share: her height and weight with an advertiser A that sells clothes, her location with an advertiser B that sends last-minute restaurant discounts, and her interest on rock music with an advertiser C that promotes rock music concerts. Under this mode an advertiser with the user's consent can keep trace of the specific interactions of the user with its ads; 3) In our solution, users are rewarded for both their interaction (e.g., watching or clicking) with ads as well as for the data they voluntarily decide to share with advertisers; 4) The current Ad Tech industry builds profiles of users based on inference techniques that use for instance the browsing history of the user. The profiles resulting from these inference techniques have been proven inaccurate [13], [14]. Also, privacy-preserving solutions like Brave or FLoC stick to the use of such inference algorithms. Instead, our solution leverages self-declared information by users. This implies strong guarantees that ads delivered to a user are very likely aligned with their preferences; 5) The use of cryptography techniques generate irrefutable proofs of the actions performed by the involved stakeholders in our solution. In other words, our solution natively integrates auditing capabilities to provide safety to users, publishers, advertisers and other Ad Tech stakeholders.

To the best of the authors knowledge, there is no other privacy-preserving advertising solution offering the described set of features. Despite this, our solution does not aim at substituting existing ones, but to offer citizens and advertising stakeholders an alternative solution that aims to increase user privacy and, at the same time, increasing the efficiency of the ecosystem sending users ads more relevant to them.

While conceptual solutions may be theoretically superior to the state-of-the-art, there are practical requirements that might

make such conceptual solutions non-operational in practice. In the context of online advertising solutions, these practical requirements can be roughly divided into two types. On the one hand, the online advertising market imposes a very strict time restriction since the ad delivery process must be completed in the order of few hundreds ms. On the other hand, ad delivery software operates in handheld devices (e.g., smartphones) which have limited resources (e.g., CPU or memory) and run on limited capacity batteries. So the misuse of such resources may severely affect the user experience. To confirm that our solution is operational in practice, we have run extensive simulations to measure the delay in the ad delivery process as well as the consumption of CPU and memory resources. Our results show that the ad delivery process is limited to tens of milliseconds for ads of standard size. Moreover, the CPU and memory consumption remains below 2.5% and 0.1%, respectively in all considered scenarios.

II. Background

In this section, we first describe the most commonly used advertising technology by modern advertising markets (programmatic advertising) and discuss what are the most apparent and inherent problems. Moreover, we describe the most relevant privacy preserving advertising solutions proposed by the industry in the recent past. Note that the research community has also contributed academic proposals in this field, e.g., [15], [16], [17], [18], [19], [20], which to the best of the authors knowledge have not been implemented as part of industrial/commercial solutions so far.

A. Programmatic Advertising

Programmatic Advertising is the common term used to refer to the online advertising solution in which the ad to be shown in the publisher's venue (webpage or mobile app) is chosen in real-time from a pool of active ad-campaigns. We make a distinction into two types of programmatic systems: *open-ecosystem* and *walled-gardens*. We explain the functionality of each of these systems next.

a) Open Ecosystem: Digital ads are shown in *publisher* venues (e.g., mobile apps or webpages). In particular, such venues offer ad spaces. Each time an ad space is available, a programmatic ad delivery process is triggered. Ad spaces are managed by the publisher's ad server, which (if available) loads a pre-configured ad in the ad space. Otherwise, it sells the ad either in a private or the open market[1]. Specifically, the publisher's ad server offers the ad space to an entity referred to as Supply Side Platform (SSP) through an ad request. This ad request includes information about: 1) the ad space (venue where it belongs, allowed type of ads, size, etc); 2) the user (e.g., age, gender, location, interests, etc.). This information is inferred through different tracking strategies (e.g., cookies, fingerprinting, etc.); 3) the device (mobile vs. fixed, Operating System, etc). SSPs typically handle ad requests from tens to hundreds publishers. The publisher along with its ad server and the SSP form the so-called *sell side* in programmatic advertising.

The SSP forwards the ad request to one (or more) Ad Exchange (AdX). The AdX gathers the information from the ad request and translates it into an OpenRTB protocol's bid request [21], which is sent to several Demand Side Platforms (DSPs). The DSPs are technology platforms where advertisers (or their agencies) configure their ad campaigns. Advertisers, their agencies and DSPs form the *buy side* in programmatic advertising AdXs are the platforms connecting the sell and buy sides. Upon the reception of a *bid request*, a DSP checks if the information it includes about the ad space, the user and the device matches any of its configured ad campaigns. If so, it replies with a *bid response* message including a bid for the offered ad space. The AdX collects all the *bid responses* from different DSPs and conducts a real-time auction to select the wining bid. The winning DSP is informed with a *win-notice* message and provides the URL from where the ad can be retrieved. Note that, ads are typically stored in either the advertiser or the DSP's ad server. Upon the reception of the ad's URL, the user's device retrieves the ad and renders it in the corresponding ad space. The advertiser that have delivered the ad pays a fee which is shared among all the involved players (publisher, SSP, AdX and DSP).

Finally, note that the programmatic ad delivery process sets strict time constrains in the order of hundreds of ms [22]. To maximize the marketing effect of ads, it is desired that the ad can be rendered as soon as possible after the webpage/mobile app loading process is triggered.

Interested readers can find a more detailed description of the functionality of the open programmatic advertising in [23].

b) Walled-Garden: We refer to walled-gardens as those advertising platforms where a single player controls the full ad delivery process. Examples of relevant walled-garden players in the online advertising ecosystem are Facebook, YouTube or Brave.

The essence of the ad delivery process is the same as in the case of the open ecosystem. In particular, the walled-garden platform owns the venue where ad spaces are shown (e.g., Facebook's application), so that they play an equivalent role to publishers in the open ecosystem. In addition, walled-garden platforms allow advertisers to configure their advertising campaigns based on the type of ad and the targeted audience and device type. Advertisers also configure their budget parameters (e.g., the price they are willing to pay per ad impression or per click). This service is equivalent to the offered by DSPs in the open ecosystem.

When an ad space is available, the walled-garden platform gathers information about the ad space, the user and the device and runs a real-time auction among those ad campaigns matching the gathered information. The auction algorithms selects a wining ad campaign whose ad is delivered to the user. Walled-gardens typically force advertisers to store ads in its own platform, so that they play the equivalent role of advertiser/DSP ad server in the open ecosystem. The fee payed by the advertiser delivering the ad goes entirely to the walled-garden platform.

[1]Both markets operate similarly. The only difference is that private markets are formed by a selected group of stakeholders.

c) Privacy considerations: The online advertising ecosystem offers a clear advantage over traditional advertising channels like TV, press or radio stations: *personalization*. People's online activity can be tracked and afterwards processed to obtain a profile of each individual, which reveals their preferences and interests. Conceptually, this is a good idea, because knowing the interests of someone allows showing them ads aligned to their interests. However, the *obsession* for improving personalization has led to the development of a sophisticated and invasive tracking ecosystem mainly motivated by the digital advertising business model. This ecosystem even goes further than the online activity of people and, with the proliferation of smartphones, it is able to also track the physical mobility and places visited by an individual [24], [25], [26], [27], [28].

This sophisticated tracking ecosystem has led to different scandals [1], [2], [3] that have triggered a reaction by people and public administrations. On the one hand, despite of the described tracking ecosystem, online advertising stakeholders still largely fail to show people ads of their interests [13], [14], which translates into many users considering online ads annoying and useless. This users dissatisfaction along with the perception of privacy intrusion have led people to increasingly install ad blocker solutions [29], [30]. On the other hand, the numerous scandals related to personal data misuse have led some administrations to develop modern data protection legislation to guarantee personal data is collected, stored and processed under clear and strict conditions. Under these new regulations, some of the standard practices implemented in the Ad Tech ecosystem may be considered illegal. Examples of these regulations are the GDPR in the EU [4]; the CCPA in California [5]; the LGDP in Brazil [31]; POPI in South-Africa [32]; etc.

The described events have motivated/forced the Ad Tech ecosystem to take action and propose few privacy preserving alternatives that we introduce in the next subsection. In addition to these solutions, there are many voices asking to eliminate the third-party cookies, which is currently the most widespread technique to conduct tracking in the web.

B. Privacy Preserving Advertising Solutions

In this subsection, we present the most relevant privacy-preserving advertising solutions proposed so far: Passive Zero-Knowledge Advertising solutions (whose most prominent representative is Brave), Federated Learning of Cohorts (FLoC, proposed by Google) and Consent-Based Personal Data Platforms (PDPs).

1) Brave: Passive Zero-Knowledge Advertising: Brave is a company whose main product[2] is the web browser with the same name. Brave browser was first released in November 2019.

The differential feature offered by Brave compared to other existing browsers is that it is a privacy-preserving browser. It blocks by default all ads and third-party trackers without affecting end-users' experience while surfing the web.

[2]Brave has recently made the release of its second product, Brave Search, in beta mode [33].

The business model of Brave is advertising. It offers their users an opt-in option to activate ads in Brave. Users opting in would receive ads. There are two important differences with respect to other browsers: 1) Brave compensate each individual Brave browser user for each delivered ad with its own cryptocurrency named *Basic Attention Token* (BAT); 2) the type of ads offered by Brave are non-invasive ads in the form of notifications that appear in the right upper corner of the screen. While significantly less intrusive than display or video ads, it is not clear the marketing efficiency of this type of ads.

Brave ads are targeted ads. The browser uses the websites visited by a person in order to infer their interests and preferences. However, this information stays local in the browser and it is neither shared with third parties nor even with Brave's own back-end. Instead, Brave collects a pool of ads from the ad campaigns available and sends them to the browser instances. Hence, the matching of the person's profile to the most suitable campaign is computed locally in the browser instance. This is a change to the current programmatic advertising paradigm in which the profile of the user is sent through several third-party platforms to reach DSPs where the match between the ad campaigns and the person's profile is executed (See Section II-A).

Due to the described functionality we classify Brave as a Passive Zero Knowledge Advertising (ZKA) solution. We consider it Passive, since the profile of a user is inferred by the browser without the *active* intervention of the user.

Another relevant aspects to highlight from Brave's operation in the context of this paper are the following ones:

1) Brave operates as a walled-garden using as venue to show ads its browser.
2) Brave offers users the possibility of proactively (opt-in) deactivating the so-called shields that will allow: (i) trackers and third party cookies operate normally, (ii) users receive regular ads. The user can enable this action for a specific website or for all websites. Users choosing this option will have a similar browsing experience as in other browsers such as Google Chrome. Although this is possible, it may be complex for non-skilled users to set up this type of privacy configurations.
3) It cannot be considered a full ZKA solution since in the standard operation of its current version it still requires revealing the IP address of the device in some cases [34]. Note that the IP address has been identified by the GDPR as Personal Data. Brave claims that they do not record the IP address or share it with third parties. Brave enables the use of IPFS [35], a p2p DHT-based solution that is still in a very early phase where few content can be accessed.

2) Google's Topics: Google announced that Chrome, which accounts with roughly 2/3 of the browsers market share [36], [37], [38], would cease the use of third-party cookies[3]. This represents in practice the end of the third party cookies, what

[3]Initially, the cessation was announced for beginning of 2022, but in a latter press release Google postponed it to late 2023.

	Opennes	Zero Knowledge	Consent Based	Active vs. Passive	Reward for users	Auditability
Brave	Walled-garden	✓		Passive	✓	✓
Google Topics	✓			Passive		
PDPs	?		✓(fine-grained)	Active	✓	
Our Solution	✓	✓	✓**(fine-grained)**	**Active**	✓	✓

TABLE I: Summary of the features offered by state-of-the-art privacy-preserving advertising proposals and our solution (the symbol ✓indicates the solution offer that property; the symbol "?" indicates that such solution may or may not offer that feature depending on the specific implementation.

has triggered an intense debate with respect to the targeting online advertising in the *post-cookie* era.

Google's initial proposal referred to as *Federated Learning of Cohorts* (FLoC) [7], [8], has been recently discarded and substituted by a new proposal referred to as *TOPICS* [39]. In this solution, the web browser (i.e., Google Chrome) computes the top 5 interests of a user every week. These interests are extracted from the browsing history of the user, based on the categories assigned by Google to the different websites visited by the user. The interests from the last three weeks are stored. So that, when a user visit a given website, the Topics API will return 3 interests, one from each of the three previous weeks. The solution provide some features to enhance privacy. On the one hand, a third party (referred as *caller* in the context of Topics) can only receive an interest from a user, if such third party has observed the presence of that user in a website classified with such a topic. To clarify this point, let us consider the following toy example: a user U with *sports* as one of the assigned topics. A third party T in the website www.shoes.com can only received U's interest *sports* if it previously watch U in a sports website (e.g., www.sports.com). On the other hand, a sixth random topic is assigned to a user every week. With a probability 5% the random topic is returned.

While Topics offers clear significant privacy improvements compare to current cookie-based targeting approach, it cannot be considered to offer strong privacy guarantees. For instance, a player able to fingerprint a user, might be able to collect the history of interests of a user along time, coming up with a large number of interests associated to a user. Moreover, if multiple players fingerprint a user, they can share the information they have learned from the user in the background. On the other hand, Google should demonstrate the marketing efficiency of Topics. Some questions that arise around this are: are 3 topics sufficient to properly target a user?; what about demographic characteristics, such as gender or age?; how accurate is the websites' topic classification algorithm?.

3) PDPs: Fine-grained consent-based advertising: Personal Data Platforms (PDPs) offer users the possibility to handle their personal data and decide which data and with whom to share it. In the context of online advertising, these platforms allow users to decide the players they are willing to share data with, and which specific data items. The result is a fine-grained consent-based form of advertising. PDPs typically offer people a user interface (e.g., mobile app), where people can configure their data-sharing preferences (e.g., which data share and with whom). Based on the users' configured privacy preferences, a PDP can offer audiences in bulk or individually (as it would occur in online advertising) to the advertisers providing all required data protection guarantees. Moreover, it is a common design choice among proposed PDPs to offer users explicit rewards in exchange of their data as, for instance, Brave does.

Fine-grained consent-based advertising and PDPs are quite recent concepts that are still being covered by research projects [12]. However, there have been already several start-ups proposing a PDP solution, e.g., [9], [10], [11].

III. Our solution

A. Context

The review of existing privacy-preserving advertising solutions allows us to define a set of features to frame the design of our solution and contribute a step forward in the context of privacy-preserving digital advertising. In particular, the features we consider in the design of our solution are:

1) *Openness*: We have seen that advertising solutions can operate either as walled-gardens, where ads are shown in a venue controlled by the stakeholder (e.g., Facebook or Brave), or in the open market, where ads are delivered in third party venues (e.g., FloC or open programmatic market).
2) *Zero Knwoledge*: Some privacy-preserving advertising proposals (e.g., Brave) allow to implement targeting advertising without sharing the user information with any third party.
3) *Consent-based*: Some privacy-preserving proposals offer users the possibility to explicitly consent which information can be shared with third parties such as the case of PDPs.
4) *Active vs. Passive*: We refer as *passive* solutions to those ones relying on inference algorithms to obtain the preferences of the user without their intervention (e.g., Facebook, Google or Brave). Instead, in *active* solutions users take an active role and explicitly declares their preferences (e.g., PDPs).
5) *User's compensation*: Some privacy-preserving solutions opt to reward the users for the ads delivered to them (e.g, Brave or PDPs) whereas others (e.g., FLoC) do not compensate users.
6) *Auditability*: The use of cryptographic techniques allow to create proofs of events related to each advertising operation or event, which in turn enables the possibility of auditing the system functionality. For instance, Brave offers this functionality.

Table I summarizes the functionality offered by each of the discussed privacy-preserving solutions in Section II across the defined features.

B. Requirements

Using the 6 features introduced before as reference, our goal is to propose a solution that meets the following requirements:

- *Open* solution able to deliver ads across any potential venue that operates (now or in the future) in the programmatic ecosystem (webs, mobile apps, TV, Outdoor screens, etc).
- *Active* solution where users explicitly declare their interest, instead of relying in unreliable inference algorithms [13], [14].
- It should implement a combination of *Zero Knowledge* and fine-grained *Consent-based* advertising. In particular, it would operate a ZKA protocol by default. However, for those specific cases in which the user explicitly provides consent to share a specific set of data items with a specific third-party, such information will be shared with the indicated third party.
- It should implement a *compensation* scheme for users in order to share with them the economic benefit resulting from the advertising operation.
- It should be *auditable*.

Table I shows the features of our solution and allows to compare them to those offered by state-of-the-art solutions introduced in Section II.

We would like to highlight that the information presented in Table I should not be consider as basis to argue a given solution is better than other. The solutions considered in the table must be understood as alternative solutions offering different features, which can very well co-exist together. The purpose of Table I, in the context of this paper, is to show in a visual and simple manner that our solution is different from state-of-the-art privacy-preserving advertising proposal from a technical and a functional aspect.

C. Assumptions

We make a number of assumptions regarding functions that we include in our proposal for which a solution already exists. Next we describe them:

- **Unique Identity linked to a physical person**: We need that each user is represented in our platform through an *Avatar* linked to a real person. To this end we leverage available technology which solves this issue, e.g., [40], [41].
- **Registration Process**: Again, we assume that the registration process is provided by some existing technology. Indeed, the same solution can provide both the identity matching (discuss in the previous bullet) and the registration functions [40], [41].
- **Smart contracts between parties**: Each time a transaction between a user and a third party occurs cryptographic non-repudiable proofs are generated. These provides auditing guarantees for each transaction. For some of these transactions, specific implementations of our solution may consider the use of smart contracts. In this case, we again propose to use existing technology that solves this problem, e.g. Smart Contracts on top of Etherum [42].
- **Auditing process**: In this paper, we just describe how to create auditable transactions, so that any implementation of our solution is subject to auditing not only by the involved stakeholders but also by third parties. The details where the auditable proofs are stored (most likely a blockchain) and how the auditing process can be implemented is out of the scope of this paper. Actually, this is something specific to each implementation.
- **Compensation to users**: As indicated above, our solution is expected to reward users for their interaction with ads. In particular, the company running our solution will compensate people for sharing their data with advertisers as well as for their interaction with ads. In principle, we assume that this compensation will be done through a cryptocurrency (e.g., Cardano, BAT, etc) but other options could be implemented as well (e.g., free subscription to Netflix).
- As for the rest of literature in the context of ZKA and Content-based Advertising (CBA), we do not address the issue of advertising fraud in this paper. However, it is worth noting that our solution significantly limits the ability of an attacker to commit fraud. As described above, each avatar in our solution must be linked to a unique real-world identity. Hence, the number of accounts an attacker can create in the proposed system is limited to the number of real-world identities it has access to, which is likely to be limited to a few accounts. This significantly increases the difficulty of creating botnets or likewise large scale attack infrastructures. Studying in detail fraud aspects is left for future work.

D. Involved Players

In this subsection, we describe the main stakeholders considered in our solution. Figure 1 shows a scheme representing the described components and their interactions.

- *Avatar*: This is the user identity within our solution. This identity must be linked to a real person's identity, but no personal data is available as part of this identity. We refer to it as person's Avatar. Each individual is armed with a certificate linked to its correspondent public/private keys. Indeed, we envision using modern solutions such as hierarchical deterministic keys [43], [44] where an arbitrary number of public/private key pairs can be generated from a seed public/private key pair. This technique is used to create hierarchical deterministic crypto-currency wallets [45].
- *Ad Delivery Software*: As described above, we envision an open and democratic solution that can operate in any third-party publisher willing to show ads in the online advertising ecosystem. Therefore, our solution will be implemented in a specific software that can be integrated by third parties. In particular, in the mobile ecosystem the ad delivery software is expected to be deployed in

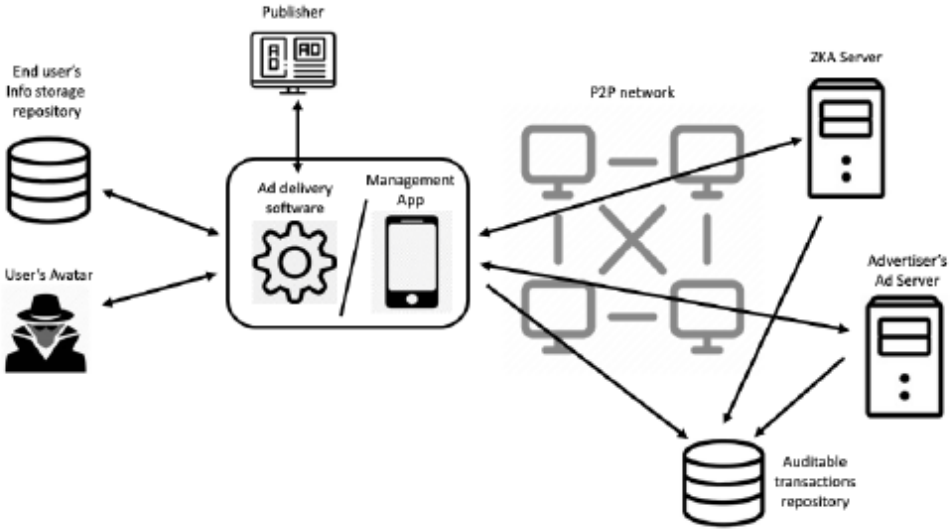


Fig. 1: Scheme of our solution including the components and the interaction among them.

an SDK to be integrated by mobile apps, whereas in desktops the ad delivery software can be either integrated within the web browser or be implemented as a web browser extension.

- *Publisher*: The publisher is the owner of the venues offering ad spaces, specifically mobile apps, web pages or video platforms. The publisher will integrate the ad delivery software described above, and this one will take care of choosing the ads to be shown in the publisher's venue.
- *Advertiser ad server*: In current programmatic advertising, ad campaigns are configured in DSPs. Moreover, ads are served from advertisers' ad servers or, if chosen by the advertiser, from its DSP's ad server. For simplicity, in this paper we consider a single entity, referred to as Advertiser ad server, that will take care of all the Advertiser related interactions. Note that, in a specific implementation of our solution, the functions offered by this Advertiser ad server can be divided across different entities. While this might impose some practical considerations, it does not impose any conceptual or design limitation.
- *Zero-Knowledge Ad (ZKA) Server*: A company using our solution will operate what we refer to as a Zero Knowledge Ad (ZKA) Server. This server will serve as intermediary to distribute the available ad inventory reported by advertisers to the *ad delivery software* installed in the user's device. It will receive only the data from the ad delivery software required to implement the billing and accounting process and will not receive any data which could reveal the identity of the user. This is why we refer to it as a *zero knowledge* ad server.
- *P2P network*: Our solution deploys a P2P network formed by users that voluntarily indicate their willingness to participate in such network. This P2P network guarantees that all communications started by user's avatar A in device D are routed through other members of the P2P network towards its final destination. By doing so we avoid any third party (Zero-Knowledge Ad Server Provider or the Advertisers Ad Servers) to know the actual IP address of the device involved in the communication. To the best of the authors knowledge, there is no other privacy preserving advertising solution providing such level of anonymity for the IP address of a user. We remind that the IP address is considered personal data by the GDPR.
- *End-users' info storage repository*: End user's data is stored in a storage repository in the cloud where all the info provided by the user as well as their transactions in the ad ecosystem (through the ad-delivery software) are stored. This repository is protected by a password and only the user can access it. Note that, other access schemes might be considered as well, e.g., based on cryptography certificates. We chose password-based protection due to its extensive use and familiarity even for non-skilled people.
- *Auditable transactions repository*: All executed transactions are cryptographically signed by the involved players and the signed probes are stored in this repository, which can be implemented using blockchain and smart contracts technology. Since all the players involved in a transaction provide undeniable proof of their agreement on the execution of such transaction, our solution provides no-reputability guarantees by default.
- *Management App*: This is the main app of the company implementing our solution. This app is the interface that allow users to: 1) configure their Avatar; 2) grant/revoke access to data to specific third parties to implement consent-based advertising; 3) access the list of transactions executed through the advertising platform (ads received, clicks on ads, etc) and the associated crypto-

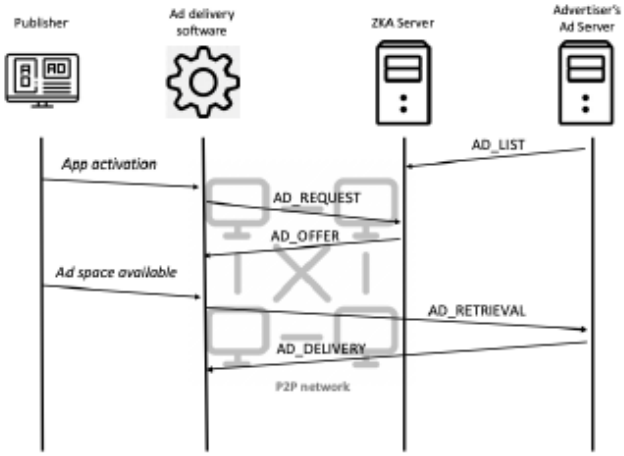


Fig. 2: ZKA protocol overview.

graphical probes; 4) have access to its associated wallet to assess the compensations received for their participation in the advertising platform. The management app is also synchronized with the end-user's info storage repository. Hence users can manage their information from multiple devices. Indeed it is expected that the management app is instantiated in the form of mobile app (so the user can use it from their mobile devices) as well as a web app (so the user can use it from any browser).

E. Protocol Description

In this section, we describe the protocol that handles the different operations to grant the desired functionality, i.e., a combination of zero knowledge and fine-grained consent-based advertising guided by the explicit instructions of the user.

We first describe the Zero Knowledge Ads delivery protocol that is the default mode of operation of our solution. Afterwards, we explain the processes involved in the fine-grained consent-based ads delivery protocol: 1) the consent granting phase, in which users can grant consent to an advertiser to access some pieces of their data; 2) the consent revoking phase, where users can revoke consent to a given advertiser to access their data; 3) the consent-based ad delivery process. Finally, we discuss the billing&accounting protocol.

1) Zero Knowledge Ads delivery: For simplicity, to describe the ZKA delivery, let us assume that the ad delivery software used is an SDK installed in a mobile app.

Figure 2 shows the exchange of messages between the different entities involved in the process. Note that, unless other way stated, each message is forwarded through a different peer that is part of a p2p network, so that the actual IP address of the user's device is never exposed to third parties (which includes the ZKA advertiser's server operator as well as the publisher and advertisers). In addition, the device use a randomly selected public/private key pair from a large pool of keys generated using a hierarchical deterministic key system. Note that the use of a single public key in all communications would make such public key an unique identifier. For the shake of readability, we avoid explicitly mentioning this in every step of the protocol. Next, we describe step by step the message exchange depicted in Figure 2.

1) The ZKA Ad Server receives from each Advertiser Ad Server an `AD_LIST` message with a list including for each ad: an *ad id* and the *ad's metadata*. The ad's metadata includes the following information: the type of ad (e.g., display, video), the size of the ad, the target audience (age, gender, interests, etc.), the IP address or URL of the advertiser ad server from which retrieve the ad, the public key of the advertiser ad server, an expiration time (the deadline to deliver this ad to users), the compensation associated with the different events related to an ad impression (e.g., a view or a click), etc. The ZKA Server collects the meta information of the ad inventory from potentially thousands of advertisers. It is part of the business strategy of the company owning the ZKA Server deciding how to process this ad inventory by aggregating it all together or dividing it in groups depending of different classification criteria (e.g., historical performance of ad inventory, preferential agreements with certain advertisers, etc.). This is not different from the strategies defined nowadays by AdXs or SSPs in the current digital advertising ecosystem.
2) Upon the activation of the mobile app embedding the ad delivery SDK software, the software creates an `AD_REQUEST` message that is sent to the ZKA Server. The only parameter included in this message is a public key.
3) Upon the reception of the `AD_REQUEST` message, the ZKA Server generates an `AD_OFFER` message formed by a list including the ad id and ad meta-information for a pool of ads selected by the ZKA Server. The `AD_OFFER` message is encrypted with the public key provided by the ad delivery software in the `AD_REQUEST` message. By doing so, only the ad delivery software will be able to access the list of received ads. Note that the ZKA Server receives neither user's data from the Ad Delivery software nor the IP address that is hidden through the p2p network.
4) Once the list of ads is available in the ad delivery software, when an ad space is available in the mobile app, the software triggers the process to retrieve an ad to fill the ad space. Note that, defining the ad selection algorithm is out of the scope of this paper. However, the ad selection algorithm should be designed such that it maximizes the probability of the user interacting with the ad. To this end, the selection algorithm should consider the user interaction with ads in the past, the user's preferences as well as the information regarding the target audience included in the ads' meta-information.
5) Once the algorithm selects an ad, the ad delivery software retrieves the IP address of the advertiser ad server from which retrieve the ad (directly from the ad meta-information or through a DNS resolution of the URL). The ad delivery software sends an `AD_RETRIEVAL`

message to the advertiser ad server. This message includes the following data: ad ID encrypted with the public key of the advertiser ad server (by doing so, even an attacker intercepting the message would be unable to know the requested ad), a transaction ID (this will be used as unique reference of this ad transaction) and a public key associated with the user's avatar certificate.

6) Upon the reception of the AD_RETRIEVAL message, the advertiser ad server responds with an AD_DELIVERY message, which includes: the ad encrypted with the public key provided by the ad delivery software in the correspondent AD_RETRIEVAL message and the transaction ID of the correspondent AD_RETRIEVAL message.
7) Finally, the ad delivery software places the ad in the corresponding ad space.

The described process just depicts the basic functionality scheme, which is subject to different improvements/modifications. For instance, the ad selection algorithm could be executed in background to create a predefined sorted list of ads, so that the ad delivery software can prefetch a number of ads (e.g., 4 ads). Upon an ad slot is available, the ad delivery software would deliver immediately one of the prefetched ads to the mobile app for showing it to the user. Using ads prefetching the ad delivery delay would be negiglible.

2) Fine-grained consent-based Ad delivery: In this subsection we provide the details of our protocol for: 1) allowing the user to grant consent to an advertiser to access and process certain data of the user. We envision a process driven by the advertisers. An advertiser makes an offer in which it indicates the data it requires from the users as well as the compensation it is willing to deliver for the data; 2) allowing the user to revoke the consent to an advertiser; 3) deliver consent-based ads.

Note that from the user's perspective, the consent granting and revoking processes involve the management app whereas the consted-based ad delivery process requires the participation of the ad delivery software instead.

As in the case of ZKA delivery, unless otherwise stated, every message sent from the management app or the ad delivery software is forwarded through the p2p network so the IP address of the user's device is hidden.

a) Consent Granting: Figure 3 shows the exchange of messages we propose to govern the consent granting process that we describe next.

1) The advertiser ad server sends to the ZKA server a CONSENT_GRANTING_OFFER including: the data requested from the user (e.g., age, gender and location or age, gender and top interests); the offered compensation in the selected crypto-currency; the advertiser-ID and its URL (in case the user want to learn more from the advertiser); the IP address of the advertiser ad server; the offer ID; a public key associated with the advertiser. Obviously, an advertiser may send more than one offer. The ZKA server collects the CONSENT_GRANTING_OFFERS from multiple advertisers.

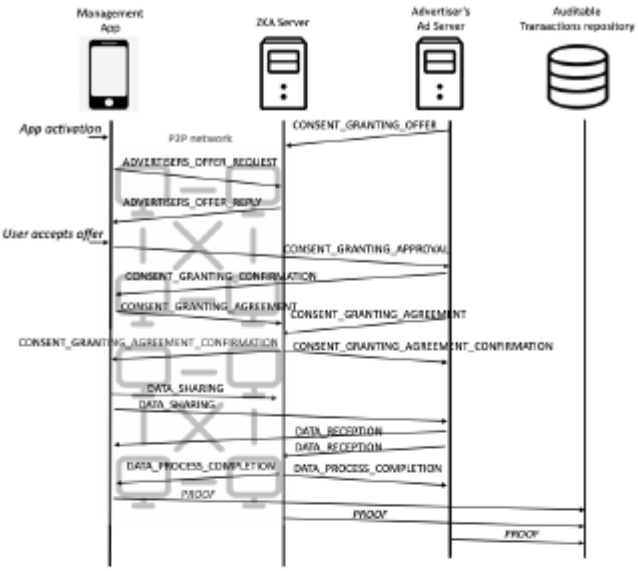


Fig. 3: Consent-granting protocol overview.

2) Upon the activation of the Management App, it sends an ADVERTISERS_OFFER_REQUEST to the ZKA server. This message only includes a public key associated with the user's avatar.
3) Upon the reception of the ADVERTISERS_OFFER_REQUEST, the ZKA ad server sends to the Management app an ADVERTISERS_OFFER_REPLY including the information of a pool of advertisers' offers. Note that the algorithm to select which offers to send to each request is out of the scope of the paper. For simplicity, we consider that all offers available at the ZKA server are included in every ADVERTISERS_OFFER_REPLY message. The message is encrypted with the management app public key, so that even if an attacker intercepts the message will not be able to read or modify it.
4) The management app processes the ADVERTISERS_OFFER_REPLY message and presents the different offers in a visual form to the user. If the user accepts an offer, the management app generates a CONSENT_GRANTING_APPROVAL message, which includes the following information: transaction ID (this is an unique ID of the transaction); a tuple formed by the offer-ID, advertiser-ID, user-ID and compensation encrypted with the public key of the advertiser. Note that the user-ID is a random number generated for the sole purpose of the relation between this advertiser and the user. Note, that the user-ID used for different advertisers is different and it is not linked to any PII data Moreover, the management app generates an undeniable proof of the consent granted by the user. To this end, it generates a token, which is a version of the previous tuple (transaction-ID, offer-ID, advertiser-ID, user-ID and compensation) signed with a private-key from the user's avatar. The CONSENT_GRANTING_APPROVAL

is sent to the advertiser ad server.

5) The advertiser ad server, upon the reception of the CONSENT_GRANTING_APPROVAL message responds with a CONSENT_GRANTING_CONFIRMATION message. This message includes: the transaction-ID as well as a token which is the signed version of the tuple introduced above (transaction-ID, offer-ID, advertiser-ID and compensation). It is signed with a private key from the advertiser. The confirmation message is sent to the Management App.
6) At this stage, and prior to proceed with the data sharing, both entities, the Management App and the advertiser's Ad Server, send a CONSENT_GRANTING_AGREEMENT message to the ZKA Ad Server. This message includes the transaction ID and the compensation information. The Management App signs it with a private key from the user's avatar and the advertiser ad server signs it with a private key from the advertiser.
7) Upon the reception of both CONSENT_GRANTING_AGREEMENT messages, the ZKA ad server sends a CONSENT_GRANTING_AGREEMENT_CONFIRMATION message to both, the Management App and the advertiser ad server. This message includes the transaction ID and compensation information signed with the private key of the company running the ZKA ad server. At this point the three involved parties have generated undeniable probes that they are aware of this transaction and approve it.
8) On the reception of the CONSENT_GRANTING_AGREEMENT_CONFIRMATION, the Management App sends a DATA_SHARING message to the advertiser ad server, that includes the data agreed to be shared with the advertiser. This message includes the transaction ID and the shared data encrypted with the public key of the advertiser ad server. Therefore, only the advertiser would be able to access the shared data. Finally, this message is also signed with the private key of the user's avatar, so that the user is providing undeniable proof that they shared such data. Hence, if the user is faking the shared data, there will be an evidence that can make the user accountable for faking the data. Moreover, the Management App sends a replica of the DATA_SHARING to the ZKA ad server without including the encrypted data part to provide even more guarantees the ZKA cannot access the user's shared data.
9) Upon the reception of the DATA_SHARING message, the advertiser answers with a DATA_RECEPTION message informing that the data has been received. This message includes the transaction ID signed with the private key of the advertiser's ad server. This message is sent to both the Ad Manager app and the ZKA ad server.
10) Upon the reception of both DATA_SHARING and the DATA_RECEPTION messages, the ZKA ad server sends a DATA_PROCESS_COMPLETION message to both the Management App and the advertiser ad server. This message includes the transaction ID and is signed with the private key of the ZKA ad server.

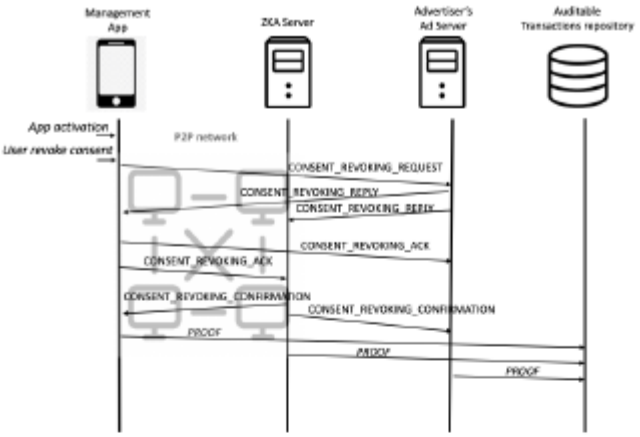


Fig. 4: Consent-revoking protocol overview.

Once the described protocol has been executed, the three entities involved in the process have agreed on the existence of the transaction and the completion of the data sharing and have generated a signed proof of their agreement. We have described an option in which the undeniable proofs consists of cryptographic proofs through signed messages that, as we describe later in the paper, are stored in the *auditable transactions repository*, e.g., a blockchain. However, other alternative approaches such as smart contracts can be also used in the described protocol with very minor modifications.

b) Revoking consent: Figure 4 shows graphically the exchange of messages that allows a user to revoke the consent granted to an advertiser to use their data.

1) When the user indicates their willingness to revoke the consent granted to an advertiser through the Management app, this one generates a CONSENT_REVOKING_REQUEST message. This message includes the transaction ID associated with the corresponding consent granting process, identifying the specific consent instance to be revoked. The message is signed with a private key from the user's avatar certificate and it is sent to both the the advertiser ad server and the ZKA server.
2) Upon the reception of the CONSENT_REVOKING_REQUEST message, the advertiser ad server sends a CONSENT_REVOKING_REPLY message to the Management app and the ZKA server. This message is signed with the private key of the advertiser. In the CONSENT_REVOKING_REPLY, the advertiser ad server also includes the data it is storing from the user and is planning to remove. This information is encrypted using the public key of the user's avatar, so only the Management app can read it.
3) The Management app verifies whether the the data to be removed is correct (it corresponds to the shared data in the consent granting process) and, if that is the case, sends a CONSENT_REVOKING_ACKNOWLEDGMENT to both the advertiser ad server and ZKA ad server. This message includes the transaction ID and is signed with

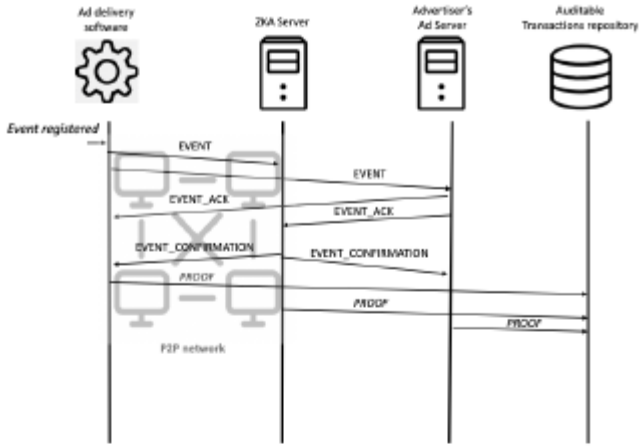


Fig. 5: Billing & Accounting protocol overview.

a private key from the user's avatar.

4) Finally once the `CONSENT_REVOKING_REPLY` and `CONSENT_REVOKING_ACKNOWLEDGMENT` is received by the the ZKA server, it generates a `CONSENT_REVOKING_CONFIRMATION` including the transaction ID, which is signed with the private key of the ZKA server. This message is sent to both the Management app and the advertiser ad server.

When the described process is concluded, the three parties have generated cryptographically undeniable proofs that they have implemented the consent revoking task. In addition, the advertiser provides proof of the data it had about the user and that it must remove due to the consent revoking process. Note that, if the advertiser does not delete the data and keeps using it after the consent revoking process has been completed, there is undeniable proof that the advertiser is exploiting personal data without the user's consent. This will represent a violation of most modern data protection regulations. Therefore, our solution would allow, for instance, data protection authorities to audit misbehaving advertisers. In our view, this is an important mechanism to discourage advertisers considering to ignore users' consent revocation.

Finally, as in the consent granting process, the cryptographical proofs can be extended to use smart contracts.

c) Consent-based Ads delivery: The consent-based ads delivery uses exactly the same message exchange described for the Zero Knowledge Advertising case. The only difference is that the ad delivery software includes the user ID (encrypted with the public key of the advertiser ad server) in the messages shared with the advertiser ad server. By doing so, the advertiser can match this ad with the specific user who granted the consent.

3) Billing & Accounting: The final function to implement is the billing & accounting process, which we address in this subsection. Figure 5 shows the messages exchange of our protocol to implements this function. Note that this process is triggered by an event associated with an ad (e.g., a user view or click in an ad). The process is the same independently of the type of event.

1) Upon the completion of an event, the ad delivery software generates an `EVENT` message including the following information: type of event (e.g., click or view), an event ID (a single identifier for the current event), the transaction ID (corresponding to the ad associated with this event), a wallet ID (the wallet where the cryptocurrency payment should be transferred) and the compensation associated from the event (extracted from the meta information of the ad). The ad delivery software signs the `EVENT` message with a private key from the user's avatar and sends it to both the advertiser ad server and the ZKA server. Note that we propose the use of Hierarchical Deterministic wallets [45], so that different transactions are associated to different public/private key pars from the wallet. The use of a single wallet ID would make this one a potential unique identifier of the users' avatar.
2) Upon the reception of the `EVENT` message, the advertiser ad server creates an `EVENT_ACK` message including the: type of event, event ID, transaction ID and the compensation associated with the event. The message is signed with its private key and sent to the ad delivery software and the ZKA server.
3) Finally, once the `EVENT` and `EVENT_ACK` are received by the ZKA server, this one generates an `EVENT_CONFIRMATION` message including the same information as the `EVENT_ACK` message. This message is signed with the private key of the the ZKA server.

It is important to note that, the consent granting also generates a monetary transaction and thus it should undergo the billing and accounting process. The process is the same as the one described above with slight modifications: the event type is consent granting and the transaction ID is the transaction associated with the consent granting process.

F. Auditability

In the previous section we have described the protocol that governs the functionality of our solution. In each of the described processes there are three involved players: 1) the advertiser ad server; 2) the ZKA ad server and 3) the ad delivery software or the management app (depending on the specific process). In every process each of these entities generate cryptographically signed proofs that confirm their agreement with respect to the process. In some cases, these confirmations include data exposing the specific activity of the entity within the process. For instance, in the consent revoking process, the advertiser ad server declares the data that it is going to delete.

The generated proof by an entity is sent to the other two entities, such that the three entities possess for each process its own proof but also the proof generated by the other two entities.

These proofs are uploaded to the *auditable transactions repository*, so that they can be validated and available in case any dispute between the parties requires so. In particular, we suggest this entity to implement a blockchain for auditing purposes.

Note that upon a dispute, e.g., a user rejecting it granted consent to an advertiser or an advertising still using data from a user after the consent revoking process has been executed, the proofs available in the *auditable transactions repository* can be accessed to settle the dispute since they provide undeniable guarantees of the actions taken by each party.

IV. Evaluation

The discussion presented in Sections II and III have made clear the main conceptual differences between our proposal and the state-of-the-art alternatives. Note that, we claim the design of our solution represents the main contribution of this paper, since it provides a new approach to deliver digital ads with full data protection guarantees, that extends the portfolio of the already existing solutions (See Table I).

Hence, since the main motivation of our proposal comes from a conceptual standpoint, and we acknowledge that our proposal is meant to co-exist with other existing approaches, a head-to-head performance comparison of our solution with the existing alternatives does not add much value to the paper. Instead, we must carefully evaluate that our solution qualifies from a technical and performance point of view to operate under the requirements imposed by the current online advertising ecosystem. As described in Section II, programmatic advertising set strict time constrains to guarantee that ads are rendered in hundreds of ms. From a quantitative performance perspective, our solution should be able to perform the complete ad delivery process within the established time constrains in the programmatic ecosystem. The equivalent to our solution within the current ad delivery process in programmatic advertising corresponds to the steps 4 to 7 of the ZKA protocol described in Sec. III-E1 and Figure 2. This is the part subject to timing constrains. For completeness, we also present timing results related to the steps 1 to 3 of the ZKA protocol, which is meant to send to the *ad delivery software* a list of available ads.

Moreover, the ad delivery software is expected to run in different types of devices from desktops to mobile phones. The use of resources (CPU, memory) is important in all type of devices but specially in mobile phones. Mobile phones operate a more limited architecture in terms of CPU and memory and use limited capacity batteries. Having this mind, our solution should make a limited use of these resources.

Finally, note that the obtained results can be generalized to the consent-based advertising alternative since the process is essentially the same, excepting few small variations in the information added in some of the messages (i.e., the user id), whose impact in the overall delay and resources consumption is negligible.

To assess the performance of our solution in the referred dimensions (time constrains and resources consumption), we have run extensive simulation experiments. In particular, in the rest of the section, we first describe the simulation setup and then we present the results obtained from the conducted simulation experiments. In particular we evaluate 3 metrics: delay of ad delivery process and CPU and memory consumption.

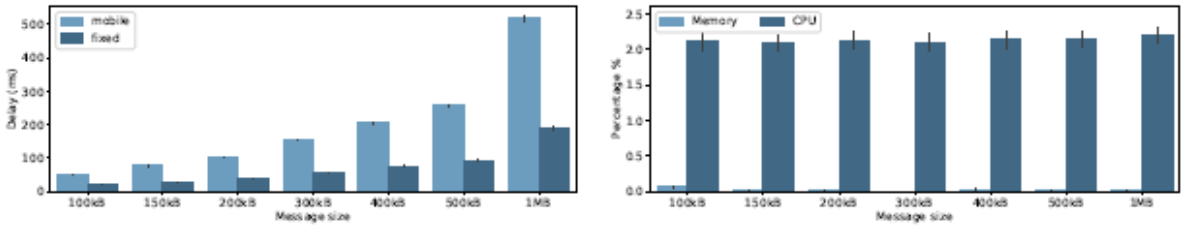
A. Simulation setup

Our simulation considers all the players involved in the ZKA delivery process: the mobile app, the ad delivery software, the ZKA server and the advertisers ad server.

The simulator has been implemented in Python. Next we detail the implementation of the different functions involved in the ad delivery process:

- We have implemented the exchange of messages using standard HTTPS/TCP sockets between the different players.
- The fields of the messages have been implemented using a serialization mechanism. This is a very common approach to encode data in Internet protocol payloads.
- To implement the cryptographic operations, i.e., encryption and signature functions we have used the Fernet library [4]. We assume a scheme URL-safe base64-encoded 32-byte key utilizing an implementation of symmetric authenticated cryptography, which is commonly used in the web.
- We have emulated the communication between the different players using an open stack infrastructure. Each player (ad delivery software, advertiser ad server and ZKA ad server) is set up in an independent open stack instance with 4GB RAM and 4vCPUs. Note that mid-range smartphones are equipped with similar resources to our open stack instances. Instead, back-end servers offer significantly more powerful resources.
- The ad selection process should happen in the order of few ms (in the worst case). Hence, we can safely assume that its contribution to the overall delay is negligible.
- We consider the advertiser ad server is hosted in a data-center owned by the advertiser or by a Content Delivery Network (CDN). In any of these cases, it is expected to account with network connections in the order of Gbps for both up and downstream.
- We assume that devices hosting the ad delivery software are end-user devices (smartphones, tablets, laptops or desktops) which could then be connected to either the fix or the mobile network access infrastructure. To simulate the download and upload rates associated to these devices we use as reference the data from the Ookla Speedtest [46] that provides the average upload and download rates for broadband fixed and mobile infrastructure across hundreds of countries. In each simulation run we select a random value for the upload (download) rate of the device from a range defined by the max and min upload (download) rates reported by Ookla for the 100 countries with fastest networks.
- Devices hosting proxy nodes from the p2p network are end-users' devices, which are selected in a smart way to guarantee good performance. To this end, in our simulation we assume that p2p proxies are end-user devices connected to broadband networks selected from the same country as the device hosting the ad delivery software. Hence, the upload and download rates of the p2p proxy

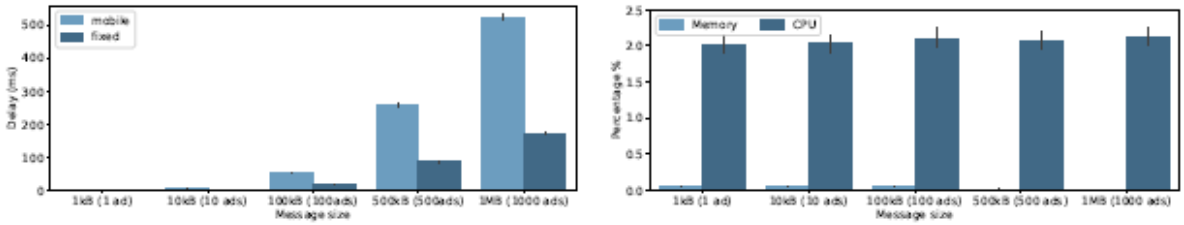
[4] https://cryptography.io/en/latest/fernet/



(a) Delay of communications

(b) Percentage of Memory and CPU consumption

Fig. 6: Performance results for steps 1 to 3 of the ad delivery protocol corresponding to the delivery of the metainformation of ads from the *ZKA server* to the *ad delivery software*



(a) Delay of communications

(b) Percentage of Memory and CPU consumption

Fig. 7: Performance results for steps 4 to 7 of the ad delivery protocol corresponding to the delivery of the ad from the *advertiser ad server* to the *ad delivery software*

would be accordingly obtained from the fixed broadband data from Ookla Speedtest.

- To simulate the effect of the p2p network, we consider a worst case scenario, in which the proxy receives the entire message from the source before forwarding it to the destination. This technique is referred to as *Stop-and-Wait* in communication protocols and it is known to be inefficient. However, in the context of our paper it serves the purpose to find an upper-bound for the delay introduced by our protocol.
- We assume that each ad metainformation register included in the `AD_OFFER` has a size of 1KB. Note that this is an upper bound of the actual expected size of the metainformation from an ad. In our simulation, we consider the `AD_OFFER` message include metainformation for N= [1,10,100,500,1000] ads.
- The common ad size in programmatic advertising is 150KB [47]. In our simulations, we consider the following ad sizes [100, 150, 200, 300, 400, 500, 1000] KB. Note that we consider sizes up to 6,66 times larger than the reference size of 150KB.

B. Results

In this subsection, we present the results from the simulations regarding the communication delay, the % of CPU utilization and the % of memory consumption for the two parts of the ZKA delivery protocol.

On the one hand, Figure 6 shows the results for the first part of the ZKA delivery protocol, involving steps 1 to 3 (See Section III-E1), which are meant to deliver a list of available ads to the *ad delivery software*. On the other hand, Figure 7 presents the results for the second part of the ZKA delivery protocol (steps 4 to 7), which is dedicated to the ad delivery process and is subject to delay restrictions set up in programmatic advertising.

Note that for each of the reported scenarios we have run 500 simulation samples. We report the average value of the considered metric (delay, % of memory consumption and % of CPU utilization) as a bar and the 95 confident interval in the form of an error bar.

On the one hand, we observe that our proposed solution meets the expected performance requirements to operate in any device and under the timing restrictions imposed by the online programmatic advertising, even when we consider the p2p proxies implement the inefficient *Stop and Wait* forwarding technique. In particular, for recommended ad sizes (150kB) the average delay of the ad delivery process in our simulations is 28.51 ms and 76.34 ms, for devices connected to fixed and mobile networks, respectively. Even in the considered extreme case with ads of 1MB (6,66 larger than the typical ad size) the average delay is bounded to 191.25 ms and 518.04 ms for devices fixed and mobile network connections, still in the range of few hundreds ms. Finally, it is worth mentioning that the use of ad prefetching techniques as described in Section III would lead to negligible ad delivery delay, since ads would have been prefetched and thus available locally in the device for each new ad space.

On the other hand, we observe that the resource consumption imposed by our solution into devices running the *ad delivery software* is affordable even for handheld devices for both the ads delivery and the metainformation delivery processes. In particular, the CPU utilization and memory

consumption are smaller than 2,5% and 0,1%, respectively, in all considered cases.

Finally, we would like to highlight that the bandwidth overhead generated by our protocol is negligible. Most of the bandwidth consumption is associated with the payload of the messages. First, the size of the AD_DELIVERY message is determined by the size of the ad (typically few hundreds KB), which is common to any ad delivery platform and not specific to ours. Second, the size associated to the AD_OFFER message including the metainformation of ads. As we have discussed before, the matainformation of an ad is expected to be encoded in registers with a size <1KB. Hence, the total bandwidth consumed by these type of messages is expected to be negligible in comparison to the overall bandwidth consumed by regular web pages and mobile apps.

V. Conclusion

Different social, political and regulatory actions have urged the online advertising industry to revisit their privacy-related practices. This has led to the development of several privacy-preserving advertising approaches.

In this paper, we propose a novel privacy-preserving advertising solution that presents a combination of functionalities that, to the best of the authors knowledge, is not offered by state-of-the-art solutions in the field. In particular, our solution is designed to operate in multiple venues (webpages, mobile apps, etc). In addition, it offers a combination of zero knowledge advertising (which does not share data from users with third parties) with a fine-grained consent based advertising (which shares with those third parties explicitly indicated by a user the specific data selected by such user). Moreover, our solution operates based on explicitly declared information and preferences from users, instead of using inference mechanisms, and compensates users for sharing their data and interact with the ads. Finally, based on cryptography technology, our solution enables full auditability.

We have described in detail the protocol that will serve as the basis for the implementation of our solution as well as evaluated its performance through extensive simulations. Our evaluation confirms that the proposed solution can be implemented in practice. On the one hand, our solution meets the delay requirements imposed by the programmatic advertising delivery of ads. On the other hand, it present a limited use of resources (memory and cpu) from those devices running it.

As future work, we plan to implement a first prototype of our solution in the next months that will incorporate the feedback received from academia and industry with suggestions to improve the design presented in this paper.

References

[1] Wikipedia., "Cambridge analytica scandal," 2018. [Online]. Available: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

[2] Wall Street Journal., "Google is fined $57 million under europe's data privacy law," 2019. [Online]. Available: https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

[3] BBC, "Digital ad industry accused of huge data breach," 2021. [Online]. Available: https://www.bbc.com/news/technology-57232253

[4] THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, "General Data Protection Regulation," https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[5] California State Legislature, "California Consumer Privacy Act," https://www.caprivacy.org/.

[6] "Brave browser," https://brave.com/.

[7] Google, "FLoC whitepaper," https://github.com/google/ads-privacy/blob/master/proposals/FLoC/FLOC-Whitepaper-Google.pdf.

[8] GitHub, "FLoC repository," https://github.com/WICG/floc.

[9] "WIBSON," https://wibson.io/en.

[10] "MyDataMood," https://mydatamood.com/.

[11] "Datawallet," https://datawallet.com/.

[12] H. E. U. Program, "PIMCITY: Building the next generation of personal data platforms." [Online]. Available: https://www.pimcity.eu/

[13] M. A. Bashir, U. Farooq, M. Shahid, M. F. Zaffar, and C. Wilson, "Quantity vs. quality: Evaluating user interest profiles using ad preference managers." in *NDSS*, 2019.

[14] P. Reserch., "Facebook algorithms and personal data." [Online]. Available: https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/

[15] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas, "Adnostic: Privacy preserving targeted advertising," in *Proceedings Network and Distributed System Symposium*, 2010.

[16] S. Guha, B. Cheng, and P. Francis, "Privad: Practical privacy in online advertising," in *USENIX conference on Networked systems design and implementation*, 2011, pp. 169–182.

[17] M. Backes, A. Kate, M. Maffei, and K. Pecina, "Obliviad: Provably secure and practical online behavioral advertising," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 257–271.

[18] L. J. Helsloot, G. Tillem, and Z. Erkin, "Ahead: privacy-preserving online behavioural advertising using homomorphic encryption," in *2017 IEEE Workshop on Information Forensics and Security (WIFS)*. IEEE, 2017, pp. 1–6.

[19] Y. Pang, B. Wang, F. Wu, G. Chen, and B. Sheng, "Prota: A privacy-preserving protocol for real-time targeted advertising," in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2015, pp. 1–8.

[20] G. Pestana, I. Querejeta-Azurmendi, P. Papadopoulos, and B. Livshits, "Themis: A decentralized privacy-preserving ad platform with reporting integrity," *arXiv preprint arXiv:2106.01940*, 2021.

[21] IAB Tech Lab, "Openrtb specification v3.0," Jun. 2020. [Online]. Available: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md

[22] Google. [Online]. Available: https://developers.google.com/authorized-buyers/rtb/start

[23] A. Pastor, R. Cuevas, Cuevas, and A. Azcorra, "Establishing trust in online advertising with signed transactions," *IEEE Access*, vol. 9, pp. 2401–2414, 2021.

[24] L. Barkhuus and A. K. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns." in *Interact*, vol. 3. Citeseer, 2003, pp. 702–712.

[25] P. Sapiezynski, A. Stopczynski, R. Gatej, and S. Lehmann, "Tracking human mobility using wifi signals," *PloS one*, vol. 10, no. 7, p. e0130824, 2015.

[26] A. Ilhan and K. J. Fietkiewicz, "Data privacy-related behavior and concerns of activity tracking technology users from germany and the usa," *Aslib Journal of Information Management*, 2020.

[27] J. L. Kröger, P. Raschke, and T. R. Bhuiyan, "Privacy implications of accelerometer data: a review of possible inferences," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 2019, pp. 81–87.

[28] Y. Liang, Z. Cai, Q. Han, and Y. Li, "Location privacy leakage through sensory data," *Security and Communication Networks*, vol. 2017, 2017.

[29] M. Malloy, M. McNamara, A. Cahn, and P. Barford, "Ad blockers: Global prevalence and impact," in *Proceedings of the 2016 Internet Measurement Conference*, ser. IMC '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 119–125. [Online]. Available: https://doi.org/10.1145/2987443.2987460

[30] "Ad blocker usage and demographic statistics in 2021." [Online]. Available: https://backlinko.com/ad-blockers-users

[31] Brazilian Government, "Lei Geral de Protecao de Dados Pessoais," http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.

[32] South African Government, "Protection of Personal Information Act," https://popia.co.za/.

[33] "Brave search," https://brave.com/search/.

[34] "Brave Browser Privacy Policy," https://brave.com/privacy/browser/.