ACROSS
Towards user journeys
for the delivery of cross-border services
ensuring data sovereignty

D2.6 ACROSS Governance framework including service design approach – Final

Project Reference No	959157 — ACROSS — H2020-SC6-GOVERNANCE-2018-2019-2020
Deliverable	D2.6 ACROSS Governance framework including service design approach – Final
Work package	WP2: ACROSS New Governance Model
Nature	Report
Dissemination Level	Public
Date	30/04/2024
Status	Final
Editor(s)	Max Kortlander, Marit Hoefsloot
Contributor(s)	WAAG
Reviewer(s)	Engineering, Tecnalia
Document description	This deliverable presents the ACROSS public stack governance model and service design approach, emphasizing values-based development, participatory design, and technology aligned with public interests. After internal implementation and reflection, the ACROSS governance framework is ready for adoption by other European digital public service developers. The document concludes with reflections on its application and potential limitations.

About

The project is co-funded by the European Commission's Horizon 2020 research and innovation framework programme. Spanning through three years, ACROSS consists of a consortium of 10 partners from 7 countries: Athens Technology Center (coordinator), Tecnalia, Dataport, Engineering, Fraunhofer, GRNET, TimeLex, The Lisbon Council, Waag and VARAM.

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use, which may be made of the information contained therein.

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	**Modified by**
v1	31/10/2023	First draft written	WAAG
v1.1	16/02/2024	Internal review WAAG	WAAG
v2	29/03/2024	Draft ready for partner review	WAAG
v2.1	19/04/2024	Document reviewed by partners	Engineering, Tecnalia
v3	25/04/2024	Document finalised	WAAG

Executive Summary

This deliverable outlines the efforts undertaken by the ACROSS consortium to address critical questions around governance and service design in European technical development. Grounded in the European Commission's vision for technology aligned with public values, ACROSS has developed and refined a public stack governance model and service design approach that encompasses a values-based foundation, open and participatory design processes, and the development of technology that is open, fair, and inclusive.

Central to ACROSS's approach is the adoption of a public stack governance model and service design approach, as first presented in D2.5 "ACROSS Governance framework including service design approach – Initial". Chapters 2 and 3 describe how the public stack model was used in ACROSS to frame considerations and processes about the project's governance around shared values and goals. Chapter 4 describes how this model could be applied in other public technology development processes and presents a tool (*Public Stack Reflection Cards*) which was developed to help facilitate this process. The paper concludes with a summary of outputs connected to this deliverable, and considerations of limitations and further potential applications of the public stack model. In particular, a public stack governance and service design approach as developed and utilised in ACROSS can help other public development projects to identify shared goals and values, prioritise citizen needs, and include citizens and other stakeholders as collaborators in design processes.

Table of Contents

List of Figures

1   Introduction

The European Commission lays out a robust vision for European technology development based on public values. There is an emerging question of how public technology development projects ought to be governed. A major challenge in this regard is the inherent complexity of technological development, in which many layers are at play – foundational values, design processes, and the technology itself. All of these layers need to be governed in order to ultimately position Europeans as autonomous citizens, rather than as subjects or consumers.

To address this challenge, ACROSS has adopted and further developed a public stack governance model and service design approach. Most broadly, this entails a process that begins with identifying a values-based foundation for technical development; implementing an open and participatory design process; developing technology that is itself open, fair, and inclusive; and culminates in technology and digital services that are aligned with public values, respect planetary boundaries, and position people (users and non-users alike) as citizens with democratic agency (rather than as consumers or subjects). This approach is further defined in D2.5 "ACROSS Governance framework including service design approach – Initial".

The work carried out in the course of this deliverable, D2.6, has made two main contributions: Firstly, completing a public stack governance and service design approach process within ACROSS; and secondly, documenting and sharing this public stack governance and service design approach so that it may be adopted and applied by other developers of public technology in Europe.

1.1   Developing a Public Stack Reflection Process with External Stakeholders

How can values and goals be translated into technical systems? ACROSS partners faced this question in relation to our own project but the question is not unique to our consortium – it is a question faced by many other developers, especially those developing public and/or values driven technology. The stakes around this question are heightened in the field of digital identity, where power dynamics around access to information, services, and (digital and physical) spaces are mediated by technical systems.

Over the project's course, ACROSS partners have developed a governance and service design approach to root our technology in shared values and goals. This uncovered that governance processes around value-driven technology tend to be loose, vague, and complicated. This is problematic: co-creative technology requires that a variety of stakeholders, including non-technical experts like citizens and policymakers, be included in the development process.

To answer this need, ACROSS partners developed the "Public Stack Reflection Cards". The cards summarise the governance and service design approach in ACROSS and present it in an actionable and accessible format to democratize the technical and legal discourse around technological governance to include non-technical stakeholders. The following chapters document the process of developing the governance and service design approach, its translation into the Public Stack Reflection Cards, and the impact of this approach on ACROSS itself.

1.2   Prior efforts and context

Uptake of the public stack[1] as a model for a governance and service design approach began with a review of existing materials related to the public stack. Prior to ACROSS, the public stack already existed as a basic model for considering technology development based on public values. In the 'Shared Cities, Smart Citizens' project[2], the public stack was used to reflect upon Hollandse Luchten (a community-based air quality data commons)[3]. ACROSS draws from this work and develops it further by using and developing the public stack as a governance model in ACROSS. This process has taken place through the following steps:

- Identified values (D2.5 "ACROSS Governance framework including service design approach – Initial") including: Interoperability, functionality, and technical completeness; citizen-led control and privacy; trust and openness; European values, laws, and ethical guidelines as expressed through the ECHR and relevant legislation such as GDPR.
- Identified (D2.3) and validated gaps (D2.4 "Report for cross-border service gap analysis – Final") including: exacerbation of inequalities; and inaccessibility and exclusion because of requirements (e.g., technical literary, administrative identity, interoperability).
- Set legacy goals (goals for the sustained legacy that we would like our project to create) during the general assembly in Bilbao, September 2022. Legacy goals include developing towards: Inclusion; user-centricity; real co-creation; establishing a single point of trust; recommendations (suggestions and policy); a toolkit for makers; awareness of digital services'' value; and a technically complete workflow for specific user journeys.
- Developed a reflection process with external stakeholders (documented in chapter 2.2).
- Revisited digital identity design dilemmas (documented in chapter 2.3).

---

[1] https://publicstack.net/
[2] https://shared-cities-smart-citizens.nl/project/governing-an-air-quality-data-commons/
[3] https://hollandse-luchten.org/

- Conducted a reflection process internally with ACROSS partners (detailed in chapters 3.1, 3.2, and Appendix I).
- Finalised the research in this deliverable, and developed a public stack reflection tool to share part of the ACROSS governance and service design approach with other developers of public technology [documented in chapter 4]).

1.3 Testing and Co-creation with External Stakeholders

Waag further developed the Shared Cities, Smart Citizens Assessment[4] into a live, co-creative reflection exercise in which developers of public technology were posed various questions to help them reflect upon which values are implicitly and explicitly embedded in their design process and technology. Waag tested this reflection exercise with external stakeholders, most particularly policymakers, developers of public technology, and academic researchers. This was conducted during several live sessions in late 2022, including:

- iBestuur Conference[5], The Hague, NL
- Dutch Design Week[6], Eindhoven, NL
- Society5.0 Festival[7], Amsterdam, NL
- Rotterdam Erasmus University lecture, BOLD Cities (Big Open Linked Data)[8], Rotterdam, NL
- Amsterdam Smart City[9] event, Amsterdam, NL

The public stack reflection process was iterated further following each of these tests with external stakeholders. Based on lessons learned from the experiences with external stakeholders, we tailored and adapted the reflection process to be conducted internally with the ACROSS team (described in chapters 3.1 and 3.2).

---

[4] https://shared-cities-smart-citizens.nl/public-stack-assessment-of-hollandse-luchten/
[5] https://ibestuur.nl/partner-live-event/publieke-waarden-beschermen-met-publieke-technologie
[6] https://ddw.nl/
[7] https://society5festival.com/
[8] https://www.centre-for-bold-cities.nl/home
[9] https://amsterdamsmartcity.com/

1.4   Revisiting Design Dilemmas in Digital Identity

In preparation for an internal reflection with ACROSS partners, Waag revisited design dilemmas in digital identity which were previously developed in the European project DECODE.

The European project DECODE facilitated research into digital identity through various outputs. One such output was the 'Wegingskader',[10] (Weighing Framework) a Dutch language publication about design choices in digital identity. The Weighing Framework lays out four design dilemmas to be handled when designing and providing a system for digital identity. These have been translated to English, updated, and elaborated upon in the context of ACROSS. They can be used to question and compare choices in design and governance of systems. The four design dilemmas are:

- **Autonomous vs dependent**: Is a system built to allow for maximum agency and autonomy for stakeholders and users? How is striving for convenience and accessibility balanced with design choices that might invite engaged, critical use to encourage 'technological citizenship', in general and especially among politicians, administrators and civil servants? Does the system provide support and functions for users in a dependent position: for example, because they are ill, or immature? Can users offer help to each other?

- **Open vs closed:** Digital services are never 'finished' – they are constantly being developed and adapted. Designers, administrators and managers must therefore be available, accessible and nearby to discuss ethical, functional and technical choices with stakeholders. Users must be able to see and assess whether parties are justified in requesting the data and have a reasonable need to do so. This creates requirements for the openness of the development process, designs, information architecture, algorithms, documentation and codebases.

- **Anonymous vs identifiable**: Because digital identity is used in extremely different contexts, there are conflicting requirements and risks. This requires a flexible system that can safely switch between anonymous, pseudonymous and identifiable transactions.[11] Some transactions require extra care and therefore extra monitoring (when minors are involved, for example). While transactions involving medical information, on the other hand, have higher anonymity requirements.

- **Decentralised vs centralised**: Limit both the responsibility of individual parties and spread systemic risk by organising digital identity in a technically, legally and administratively

---

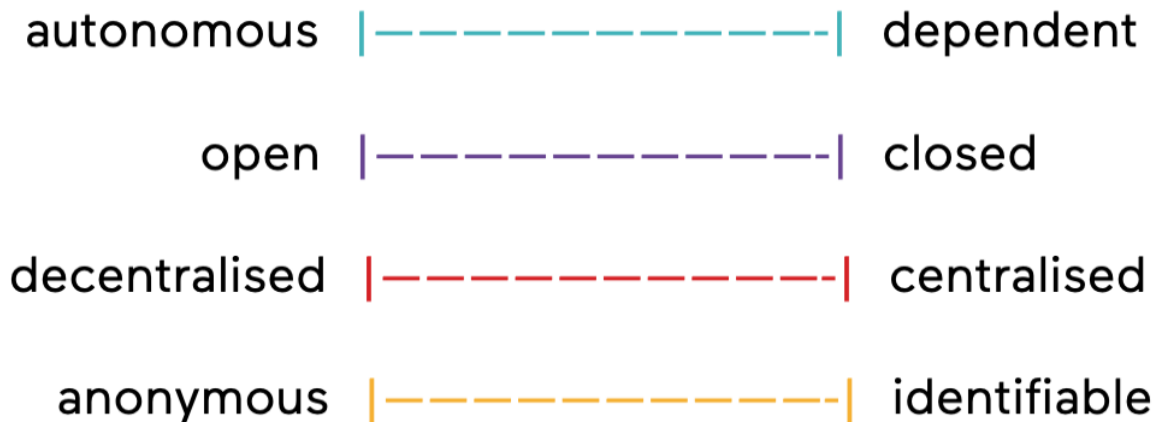[10] https://waag.org/sites/waag/files/2019-01/Wegingskader-digitale-identiteit.pdf
[11] Anonymous does not (necessarily) mean participants in a transaction are anonymous, It refers to the impossibility for third parties who are not part of the transaction to look into the transactions, even at the metadata level.

decentralised manner. At the same time, organise sufficient interoperability with central agreements, standards and supervision.

autonomous |————————————-| dependent

open |————————————-| closed

decentralised |————————————-| centralised

anonymous |————————————-| identifiable

Figure 1: Developers of digital identity solutions will encounter these design dilemmas. Our approach to governance encourages developers to find the right balance by moving to the 'left' to the greatest extent possible.

Above, the digital identity dilemmas are presented on axes as a continuum. The axes can be combined into quadrants. Design choices can then be compared with the impact they have on each dilemma. In general, for systemic reasons, a design choice leaning to the left is preferred over right, but this is highly context dependent. E.g., if your friend is sick and you want to help them, a system with easy delegation and fool proof user flow is more needed than in other cases. So: the system should be designed as left as possible, but in a given context the system should be able to move to the right where and when needed.

These design dilemmas were incorporated into the governance and service design approach in ACROSS and serve as a useful framework for other projects working in digital identity in a European context. The purpose of these design dilemmas is to encourage developers to move as far to the 'left' as possible (be as open, decentralised, anonymous, and user dependent as possible) while also acknowledging that certain contexts may require a centralised, identifiable, or automatic approach. Developers are thus challenged to find creative ways to achieve the right balance.

There are various ways in which these design dilemmas play out in ACROSS. For example:

- Centralised vs decentralised – Lists of services are centralised in the service catalogue; however, there is a federation of catalogues which is relatively more decentralised. This balance allows for

a certain level of consistency between pilots, but also allows for each pilot to tailor their own service catalogues to fit the needs of their specific context.

- Centralised vs decentralised – The user front end is relatively centralised, as all users can access it the same way through the ACROSS platform. However, user data is decentralised, because no personal data is stored locally by ACROSS. This avoids security breach and helps to protect user privacy.

- Anonymous vs identifiable – The consent and transparency dashboards strike a balance between making users identifiable where needed (by noting which data is mandatory for service providers) and allowing them to be anonymous where possible (by allowing users to choose whether or not to consent to optional fields).

- Anonymous vs identifiable – While not technically supported by ACROSS, the use of attribute-based credentials within a digital wallet was researched by ACROSS partners as a way to balance identifiability with anonymity, as such systems ideally support users to share no more personal data than is strictly necessary in a given transaction.

- Open vs closed – ACROSS's source code is open and utilises a copyleft license. Within this range, however, some of the technical components used by ACROSS are relatively more permissive, and others more restrictive. For example, much of ACROSS's technology conforms to the Apache 2.0 which is very permissive; the service catalogue uses AGPL v3 which is relatively more restrictive despite still being copyleft.

- Autonomous vs dependent – For some users, privacy is more important and they want to have the option to revoke data. For other users, automatic functions are preferred to make usability easier. This is why the consent and transparency dashboards allow for both sharing data and revoking consent. Users can by default give consent to mandatory fields but have the option to revoke all consent to any optional fields. Even if a user has given permission, they always have the right to revoke consents.

As described further in Chapter 3, these design dilemmas are also included as a tool for external stakeholders to help them identify design dilemmas they will face, and to encourage them to adopt approaches that promote openness, decentralisation, anonymity, and user dependency to the greatest extent possible.

2 Execution and Outcomes of the Public Stack Reflection Process in ACROSS

2.1 Preparing the Public Stack Reflection Exercise in ACROSS

The development and testing of a public stack reflection exercise revealed that development teams generally face difficulty in bringing governance and service design approaches 'down-to-earth' – that is, it is difficult to make governance and service design approaches actionable, particularly for non-technical experts. The interactions with external stakeholders also indicated that the public stack is useful as a tool to bridge this gap, demonstrating its usefulness for including non-technical stakeholders in reflection, deliberation, and decision making about technical design choices.

We tailored the reflection exercise developed with external stakeholders into a more detailed exercise designed specifically for ACROSS. This involved reviewing all project deliverables and meeting with partners to develop specific questions, based around input from external stakeholder sessions and the design dilemmas in digital identity. We defined a values-based foundation for ACROSS based on previous project deliverables (specifically D2.1, D2.3, D2.4, and D2.5; as well as D3.1, D3.2, D3.4, D3.5). This foundation includes:

- Interoperability, Functionality, and Technical Completeness
- Citizen-led Control and Privacy
- Trust and Openness
- European values, laws, and ethical guidelines as expressed through the ECHR and relevant legislation such as GDPR. (D2.5)

The reflection exercise spurred project partners to reflect upon how various aspects of the ACROSS design process and technology align with the values and goals set forth by project partners. The basis of this reflection exercise can be found in Appendix I.

2.2 Outcomes of the Public Stack Reflection Exercise in ACROSS12

We conducted the reflection exercise in ACROSS during the Plenary Meeting in Hamburg (Feb 2023). This exercise identified the following:

---

[12] A version of this subchapter was also presented in an ACROSS periodic progress report.

- **Alignment around shared and public values:** ACROSS partners are strongly aligned in ensuring that values identified earlier in the project (protection of digital identity, control and privacy over personal data, data minimisation) are adhered to via ACROSS's design process and technical development.

- **Identification of contextual limitations for cross border services in utilising certain types of PETs (privacy enhancing technologies):** Certain limitations arise from the context of cross-border services more generally: In this context, ACROSS partners' ideal outcomes are in some cases out of our control and reliant on service providers' willingness and capacity to adopt certain practices or technologies. For example:

  o ACROSS can only facilitate direct transfer of data from citizen to service provider (without going through ACROSS) if the service provider has an appropriate API.

  o ACROSS can only work with attribute-based credentials to the extent to which these are trusted and accepted by service providers. This raises the question: What can be done to encourage service providers to accept credentials and also limit the amount of data they request? In this regard, what can be done by service providers? ACROSS and other similar projects? Lawmakers and regulators? (These questions are explored further in chapter 5).

  o This implies that our own data minimisation practices are dependent upon service providers and marks a boundary to what can and cannot be accounted for by a technical development project's governance and service design approach. This phenomenon is considered in depth through the blog, "Service Providers Request Too Much Personal Data",[13] presented in a slightly adapted version in chapter 5.

- **Identification of challenges to address:** The reflection process has confronted ACROSS partners with specific challenges related to the technical implementation of certain values. For example, ACROSS aims to have revocable consent for the use of personal data (described further in D3.7 Legal Report). However, revoking consent requires an email to be sent by the owner of that personal data, which is something that ACROSS cannot do on a users' behalf. We identified that one functionality to aid in revoking consent could be to include a prompt (which appears when a user clicks to remove permissions to their data) explaining that users must send an email to revoke data and providing a template email message to request the removal of data. This finding may be more widely applied by other services when seeking a user-friendly way to enable citizens' revokable consent of the use of storage of their personal data. Other options include issuing

---

[13] https://waag.org/en/article/service-providers-request-too-much-personal-data/

revocation tokens by default whenever consent is given; or to require consent to be refreshed within a limited amount of time (and thus consent is automatically revoked if not refreshed).

2.3 Impact of Governance and Service Design Approach on ACROSS project and technology

The governance and service design approach enacted through WP2 efforts have taken place over the course of the ACROSS project. This was facilitated most directly through live sessions and workshops during consortium meetings and was further bolstered via remote collaborations during the times between physical consortium meetings. Taken as a whole, the impact that the efforts in T2.3 have had on the ACROSS project and technology most directly involve the prioritisation of citizen-centricity (user centricity) in terms of privacy and consent.

When ACROSS partners began development, there was a shared agreement that we "didn't just want to be another platform" and instead sought to provide a particular contribution to the field of digital identity services in Europe. As the project progressed, our consortium rallied around citizens as a prioritised stakeholder group, based on the public stack approach which views users of digital identity services as 'citizens' rather than 'consumers'. We thus identified specific design processes and technological solutions that protected user privacy and afforded users with more granular and revocable consent over sharing personal data. These include, for example:

- **Consent options beyond service catalogue requirements:** An early option for ACROSS developers was to base our work upon the basic standards for compliance as defined by service providers. The focus on user (citizen) centricity, fostered through input gathered through participatory methods via pilot partners, revealed that the basic requirements identified by service providers was not enough to provide useful information to citizens about what they could access through services and what services were requesting from them. We thus took the step to identify what was 'optional' vs 'mandatory' personal data to be used by service providers, which allows citizens more control to give consent about which data they share.
- **Prioritisation of citizen-needs in project management**: Interactions with citizens (e.g. user interviews) and internal sessions and workshops around the ACROSS service design approach shaped development requirements (e.g. KPIs, Trello tasks) to prioritise citizen needs consistently at various stages throughout the design process.
- **No centralised storage of personal data:** The decision to not centrally store personal data in the ACROSS platform directly rose from internal workshops where ACROSS partners sought to define

how to technically implement values like citizen centricity, privacy protection, and decentralization. While this design choice helps ACROSS technology to align with core values identified by partners, it also has the added benefit of simplifying our compliance with GDPR and other personal data regulations.

- **Development of transparency dashboard**: The governance and service design approach identified that interoperability and trust are central in ACROSS, both for adherence to the once only principle, and for user privacy and data control. Because of this, the consortium wanted to enforce the privacy of personal data. This led to the development of the transparency dashboard which allows users to grant or deny consent to sharing optional personal data.
- **Federation of service catalogues**: D2.3 and D2.4 identified the gap of 'trust between countries', and this informed the requirement to have a federation of service catalogues, so that pilots can manage unique and specific services without reliance on the central service catalogue. The central service catalogue, on the other hand, allows for the harmonisation of services that are shared across the various pilots.

In a reflection exercise at the final General Assembly, the ACROSS partners reflected on how the design values we agreed upon at the beginning of the project are visible in the work we have done. These included:

- **Privacy/data minimisation/data ownership**. This is visible in the transparency dashboard, data governance framework and the fact that the ACROSS platform does not store any personal data of the users. However, this value also important in the virtual assistant application, which led to the use of encrypted connections.
- **User-centricity/user-friendliness**. This value was one of the key design objectives for many ACROSS components, including the virtual assistant, transparency dashboard, user journey modelling tool, and the overall clarity and ease of the citizen front-end. However, it was also a leading value in the methods we employed as the pilot partners researched the needs and desires of the citizens and other stakeholders, which laid the foundation for the design of the platform. Moreover, a recent addition to the platform is the integration of an accessibility tool, which allows the citizen to use screen readers, change the size, font and contrast of the text, and other adjustments that facilitate the user experience. Additionally, to increase the accessibility and inclusion, we made explanatory videos and demos to explain the platform and how to use it.
- **Decentralisation**. The basis of ACROSS is a decentralised platform, i.e. it does not store any personal data but facilitates data sharing with other parties in a secure and transparent way. This

gives the citizens full control over their data, while still providing a useful service of combining different information sources, services, and steps in the workflow on one platform.

- **Interoperability.** This value led to an interesting reflection, as the partners realised that the goal of interoperability ought to be reframed. Instead of interoperability, the partners believe that common standards, agreements and protocols are the solution. This is what the ACROSS platform is built on.

- **Raise awareness about the value of EU digital services.** The ACROSS partners have presented their work in different formats, including accessible blogs; expert and citizen workshops; academic articles in journals and conferences; policy events and briefs; and online and offline toolkits to help other service providers implement our methods. This helped spread the word about the need, challenges and solutions regarding the development of EU digital services.

3 Documenting the Public Stack Reflection Process as a Resource for Others

Following a fruitful internal public stack reflection exercise with ACROSS partners, Waag developed a tool that allows others – particularly, but not exclusively, developers of public technology in Europe – to conduct their own public stack reflection process, as a means of sharing the ACROSS governance and service design approach. The questions and process from the internal reflection were iterated for a final time, to be widely applicable to a large range of development teams who are interested in building technology that aligns with public values.

The initial concept for this tool was to develop an online form with questions that would help development teams to reflect on their own governance and service design approach. Following testing with ACROSS partners and (non-ACROSS) Waag projects, we identified the need for a tool that facilitates live, collaborative, in-person discussion. For this reason, we shifted our approach and developed this tool as a set of cards (see figure 2), to be used together with a team, in a live setting.

The public stack reflection cards guide users through the governance and service design approach utilised in ACROSS. Users begin by identifying their foundation – in particular, those shared and public values which ideally drive their development process. After identifying shared values, users are then prompted to reflect on how those values are implemented in their design process and technology. The cards also prompt users to reflect upon the impact that their project has upon society (people and the planet), and to identify which design dilemmas they face that require a thoughtful balance.

The cards were first shared with various external stakeholders during the Public Spaces conference in Amsterdam (27 and 28 June, 2023). The cards are also available as a downloadable open-source tool on the public stack website[14] and in the ACROSS toolbox.[15]

---

[14] https://publicstack.net/cards/
[15] https://joinup.ec.europa.eu/collection/sipg/solution/across-toolbox/document/public-stack-reflection-cards

Figure 2: Public Stack Reflection Cards

4   Case study: data hungry service providers

There are limits to what a governance and service design approach can and cannot influence. While a project team may define certain technical choices based upon shared values and goals, certain contextual factors beyond a project's control will also influence a project's design choices.

This case study into data requests by housing providers illuminates the boundaries of what can and cannot be governed in the service design approach like that in ACROSS. The case study notes how technical development to protect privacy and data minimisation is hindered when service providers request too much information in order to establish trust. A slightly modified version of this chapter is also published as a blog "Service Providers Request Too Much Personal Data" on the Waag website.[16]

When a person moves across European borders, they must provide a large amount of their personal data to service providers including housing companies, banks, and public authorities. Essential service providers request such large amounts of personal data in order to establish trust – for example, trust that a person will consistently pay their rent on time, or trust that a person will not damage an apartment. However, this method of establishing trust is out of line with the EC's approach to personal data privacy and data minimisation: Article 5(1)(c) of the GDPR and Article 4(1)(c) of Regulation (EU) 2018/1725, which states that requests for personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[17]

According to European law, requests for personal information must be minimised and limited to what is strictly necessary. In practice, however, we find that service providers request data to establish trust, but in doing so, go far beyond the boundaries of what is strictly necessary and respectful of privacy.

4.1   Housing agencies and other service providers request too much data

It is not easy to find a new house for anyone. For people who are moving to a new country, like those who we work with in ACROSS, accessing basic services can be a data privacy nightmare. For example, a housing application in Amsterdam requires:

- Copy of ID
- Statement from employer

---

[16] https://waag.org/en/article/service-providers-request-too-much-personal-data/
[17] https://edps.europa.eu/data-protection/data-protection/glossary/d_en#:~:text=The%20principle%20of%20%E2%80%9Cdata%20minimisation,necessary%20to%20fulfil%20that%20purpose.

- Payslips from the last 3 months
- Certified copy of employment history and wage data from the Employee Insurance Agency
- Copy of bank statement showing the last salary received
- Copy bank statement showing current rent/mortgage payments
- One bank statement of the bank account from which we will collect rent automatically
- Proof of basic registration (from the municipality)
- Recent landlord declaration from current landlord
- Copy of bank cards of all tenants

This means that in order to apply for a house (without the guarantee of being selected amongst many applicants) a person is required to share their residency status, photo, date of birth, nationality, sex, and full name, immigration number, employer, salary, banking details and other personal finance information. This also requires applicants to notify their current landlord that they intend to leave. It is not clear how this information is used, how long it is held, or who has access to it.

4.2   Why is requesting too much data a problem?

There are various inherent and potential problems that result from service providers requesting too much data:

- **Invasion of privacy** – Europeans have a right to privacy under Article 8 of the European Convention of Human Rights.
- **Legal risks** – In gathering personal data, service providers become liable for potential violations to GDPR and other data protection laws.
- **Security risks** – The more that data is shared, the more vulnerable it is to falling into the wrong hands, for example through leaks, hacks, and cyber-attacks.
- **Exclusion and profiling** – Over-requesting of data excludes people who do not have access to required documentation, which can be especially problematic for people moving to a new country. Personal data can also (deliberately or inadvertently) profile and exclude people on the basis of factors like nationality, sex, age, and income.
- **Coerced consent** – People should have the freedom to decide when and with whom they share their data. Power imbalances often remove this choice for desperate housing seekers, who are compelled to share whatever data is requested.

Again, requesting large amounts of personal data is the means by which service providers establish trust. What may be constituted as 'necessary' for this purpose is a subjective matter, but there are ways to gain trust that do not require such invasive personal data exposure. As explained below, digital credentials are a technically feasible approach to minimise personal data exchange; however, these and other data minimisation practices have not yet been widely adopted by service providers who lack resources and incentives to implement them.

4.3   Attribute-based credentials may help, but cannot solve the problem

ACROSS, MGOV4EU, and other European research projects are exploring attribute-based credentials[18] as a way to protect data minimisation, privacy, and control over one's own digital identity when information is shared with services providers. Attribute-based credentials are a digital way to share no more data about yourself than is needed in a specific scenario. For example, the DECODE project illustrated a schema describing how a group people from a neighbourhood might issue a credential that vouched for someone's residency there. This credential would then be used to access an online neighborhood platform without any additional identification (not even the name of the credential holder). While technically feasible, use of attribute-based credentials is not widely implemented.

We can imagine a scenario in which attribute-based credentials are applied to requesting and sharing data as part of a housing application process. A trusted third party (like the government, an employer, or a previous landlord) issues a single credential to a person, who is then certified as 'yes, the holder of this certificate is eligible to rent an apartment within *x value range*'. The person could then present this single credential to a housing agency to verify their rental eligibility, while maintaining privacy over personal data about their identity, employment, finances, and more. Another possibility could be to utilise multiple credentials; for example, that the credential-holder is 'at least *x* years old,' or 'a legal resident', as issued by the government as a trusted third-party. Sharing multiple credentials in this way could offer some improvement from the status quo, but still carries risks related to over-identification.[11, 12] Requesting and sharing certain credentials can nonetheless still expose personal information, or wrongfully exclude certain people from consideration.

Attribute-based credentials and other technical solutions can facilitate interactions that minimise data sharing, but they do not directly address the underlying problem of trust. In our current context, service

---

[18] https://waag.org/en/article/accounting-human-agency-european-digital-identity/

providers are more likely to trust (and prefer) multiple primary sources of documentation, like bank statements, over minimised credentials.

4.4   Who can address the problem of over-requesting data, and how?

Service providers, like housing agencies, have the primary responsibility and capability to address the problem because they are generally the party that makes the decision to request too much personal data. Service providers likely over-request data for a number of reasons, including perceived risk mitigation; lack of trust in single sources of information; because nobody is stopping them; because they've become accustomed to the practice; or to filter out applicants who lack the willingness or capability to complete the extensive and invasive application process. Operating in a competitive, high-demand, and for-profit environment in which they have leverage over desperate clients like housing seekers, these service providers lack incentive to minimise data requests.

Policymakers and regulators thus have a responsibility to incentivise housing agencies and other service providers to request less data. Policymakers can regulate what can and cannot be requested by service providers in specific situations. Current legislation like GDPR, DSA, and DMA can be better enforced. Government bodies can implement privacy-by-design requirements in the technology they fund, and can provide resources and support to help service providers comply with the laws and spirit of data protection regulations.

Citizens are not responsible to address the problem, but they *are* negatively affected by it. People who are moving (and especially those moving to a new country) are generally not in a position to refuse opportunities from a housing company, bank, or other essential service provider on the basis of data privacy – they have to 'take what they can get,' and there simply are not enough alternative options to do otherwise. It is possible that people moving to a new house might collectivise in some way to demand better from service providers – but in reality, a person in the midst of moving is likely far too busy to take on the role of a data rights advocate, and it seems unfair to also place such a heavy political burden onto the general public. Citizens who are passionate about such issues might consider becoming early adopters and beta-testers of new technologies such as wallets, in order to help improve specific applications and raise awareness and demand for privacy-focused technology in general.

ACROSS and other publicly funded projects have an inherent mission to advocate for public interests. ACROSS (which helps people moving to a new country to identify the right service providers) could address the problem of over-requesting data via the technology that we build; for example, by filtering out service

providers that do not comply with strict guidelines for requesting data. While this is already done to an extent (service providers must meet technical and legal requirements as defined in project deliverable D4.2 and other technical reports), it is not realistic to find a sufficient number of service providers that would meet our ideal expectations of data protection. Furthermore, ACROSS does not have the necessary market clout to encourage service providers to adopt better practices by excluding them. It is nonetheless worthwhile for ACROSS partners to identify further ways to encourage service providers on our platform to adopt more robust data minimisation practices, and to share our findings about the contextual factors inhibiting data minimisation.

4.5   Public research projects as platforms for citizen inclusion

A strong option for future research in other public technology projects is to provide a public platform to debate, discuss, and raise awareness about issues surrounding personal data protection. Developers of public technology can advocate for citizens' rights to data protection by bringing them into the fold along with service providers and policymakers.

What do citizens want for their own data? What do they want to change about the current landscape of data sharing in Europe? How can people moving across borders work as a community to support one another and strengthen their position in relation to service providers and policymakers? What do they want their role to be? Such questions can inform future research to explore how citizen participation may help to protect personal data.

5   Conclusion

5.1   Summary of Outputs

Several outputs were developed in the course of this deliverable and Task 2.3:

- Public Stack Reflection Exercise (Internal, ACROSS Consortium. See Appendix I).
- Public Stack Reflection Tool (See Appendix II).
- Blog: *The Public Stack: a Model to Incorporate Public Values in Technology* published at Amsterdam Smart City.[19]
- Blog: *Service Providers Request Too Much Personal Data.*[20]
- Contributions to ICEGov23 Conference Paper *A more inclusive Europe through personal data sovereignty in cross-border digital public services*.[21]

Various impacts of the governance and service design approach upon project and technical decisions (primarily to drive a citizen-centred focus).

5.2   Considerations and options for further research

The public stack was further iterated and shared as the governance and service design approach in ACROSS. This governance and service design approach helps developers to understand what should be governed; it does not necessarily indicate *how* to govern. While this governance and service design approach does indeed give general guidelines, such as basing decisions upon foundational values and utilising open-source technology, the model helps developers raise specific questions, but does not answer those questions for them. This responsibility lies with developers themselves.

This governance and service design approach helps to root development process in public values, and as such is particularly relevant for European development towards eIDAS and the Single Digital Gateway. Large European technical development projects like these need to ensure that public values form their basis and are present in their technology. As ACROSS has demonstrated, the digitisation of access to public and private service providers goes beyond questions of functionality, and instead is a matter significance for society and democracy. In order to protect the openness, transparency, and accessibility of democratic

---

[19]https://amsterdamsmartcity.com/updates/news/the-public-stack-a-model-to-incorporate-public-values-in-technology-again

[20] https://waag.org/en/article/service-providers-request-too-much-personal-data/

[21] https://dl.acm.org/doi/abs/10.1145/3614321.3614329

institutions, it is thus also necessary to protect the openness, transparency, and accessibility of the digital systems which enable and facilitate interactions with those institutions.

6 Appendix I: ACROSS Internal Public Stack Reflection Exercise

February, 2023 Consortium Meeting in Hamburg

6.1 Explanation of the Exercise

- Process
  - o We have already identified shared values; gaps; and legacy goals.
  - o Now, we will do a reflection exercise in the consortium to check how well our progress aligns with our aspirations.
  - o Then, we decide if we want to do it 'externally' as well
    - E.g., with citizens, service providers, public admins

- Note: We will not get 100% of the objectives. We note what we have achieved, and also make suggestions about the way forward. This can be part of the toolbox.

- Instructions
  - o Break up into 4 groups (4-6 people per group, with technical and non-technical partners in each group).
  - o Answer the following questions per group:
    - Group 1: Tech layer, data questions (1-6)
    - Group 2: Tech layer, specific questions (7-10)
    - Group 3: Design layer, general questions (1-5)
    - Group 4: Design layer, user journey + specific questions (6-11)
  - o After a short break, we will have a plenary discussion to:
    - Address additional questions for all partners
    - Discuss any further ideas, thoughts, questions, or next steps

6.2   The Foundation

Based on a review of previous deliverables, we identify the following core values in ACROSS's foundation:

- **Interoperability, Functionality, and Technical Completeness**
- **Citizen-led Control and Privacy**
- **Trust and Openness**
- **European values, laws, and ethical guidelines** as expressed through the ECHR and relevant legislation such as GDPR. (D2.5)

Keep these values in mind as we reflect on the questions below.

6.3   Tech Layer

6.3.1   Data Questions (tech layer)

1. What personal data **passes through** the platform?
   - For what purpose?
   - Where does it go? (With whom is it shared?)
2. What personal data is **stored** by the platform? Do we keep any centralised personal data (and where, for what purpose, and under which conditions)?
3. Who generates this personal data (that is stored and/or passes through the platform)?
4. How is consent obtained and managed?
5. How do we actively protect users' personal data?
6. Briefly sketch our data flow. How is this data flow in line with our values? How is this data flow not in line with our values? Where could it be improved, and how?

6.3.2   ACROSS-specific Questions (tech layer)

1. D1.4 reads: "the second strand related to the data collected from stakeholders (users and also service providers) will be aggregated into data sets that will comprise statistical and therefore anonymous data and will be used as part of the implementation of the different key results established in the project." Is there any such data collected from stakeholders? If so, what data, and for what purpose? How are stakeholders in control of sharing this data - how is consent managed?

2. D3.1 reads: Section 3.2.5: "The framework will expose a set of APIs to be used by the Service Provider services that are going to be integrated in the framework. This API will allow the service to check the service linking status, the consents associated to end users and to inform the framework the usage of personal data." What exactly is shared in this regard? Could it potentially pose any threat to privacy or personal data control? How is consent granted and managed by relevant parties?

3. Section 6.1.1 reads "Depending on the extent in which the MyData model for personal data use and management is incorporated in the data governance framework of ACROSS, this would require a Mydata operator." **Do we have a MyData operator?**

4. What external (i.e., not project partners) checks are there on ACROSS's governance policy and its technical implementation? Which stakeholders are or are not involved in evaluation, and how?

6.4   Design Layer

6.4.1   General Questions (design layer)

1. What methodologies are used?
2. Who facilitates co-creation? Who is included?
3. What is maximised through the design?
4. What mandate does the general public have to govern the design process?
5. How is transparency assured in the process?

6.4.2   User Journey Questions (design layer)

1. Who is included represented in user journeys?
2. Who is excluded or not represented in user journeys?
3. Who can use the technology/service? Do they use the technology/service in isolation, or as part of a group/community/network?

6.4.3   ACROSS-specific questions (design layer)

1. How are citizens enabled to advocate for their rights and interests (e.g. to minimise requests from service providers)?

2. In what capacities might citizen users (of ACROSS) form a support network for one another? What would they be interested in and willing to contribute? How might ACROSS facilitate this?

3. What does ACROSS do to encourage service providers to follow better (more secure, private, minimised) data requesting practices?

6.5 Questions for the whole group (plenary discussion)

1. Where do we see overlap between the two layers?

2. Where are the design process and technical layer in line with our project's foundation in terms of the following? (Which design process and technical decisions have been made to ensure the project adheres to the following values in the foundation?):

   a. Interoperability, Functionality, and Technical Completeness

   b. Citizen-led Control and Privacy

   c. Trust and Openness

   d. European values, laws, and ethical guidelines

3. Where does the design process struggle (perhaps due to time, budget, context, or technical feasibility) to fully adhere to the following values in the foundation?

   a. Interoperability, Functionality, and Technical Completeness

   b. Citizen-led Control and Privacy

   c. Trust and Openness

   d. European values, laws, and ethical guidelines

4. How can we maintain and improve connections between technical and non-technical partners in ACROSS?

6.6 Opportunities for further reflection

1. **Pilots:** are you already using some kind of (government or other) assessment of your technology? If so, what type of assessment? What insights are gathered through it?

2. It is recommended that at least one partner conduct the TIMAPS assessment survey[22] (approx 30 minutes) as an addendum to this technical reflection. What insights are gathered from the TIMAPS assessment survey?

---

[22] https://ec.europa.eu/eusurvey/runner/TIMAPS_v_1_2_0?startQuiz=true&surveylanguage=EN

6.7   Endnotes (ACROSS Internal Public Stack Reflection Exercise)

Interoperability, Functionality, and Technical Completeness are identified in part from:

- (gap) fragmentation and lack of completeness (D2.3)
- (gap) lacking or incomplete technical infrastructure and issues related to authentication, personal data, and digital identity (D2.3)
- usability and technical completeness (D2.3)
- to have a sustained outcome (D2.5)
- focusing on the development of specialised, open, and reusable modules (rather than an all-inclusive platform) (D2.5)
- legacy goals

Citizen-led Control and Privacy are identified in part from:
- the core problem of a lack of citizen-led control (D2.4)
- privacy (D2.4)
- and enhancing data ownership and digital identity control for citizens themselves (D2.5)
- user-centricity, data sovereignty for citizens, and privacy protection (D2.5)

Trust and Openness are identified in part from:
- safe, inclusive, and trustworthy ecosystem (D2.5)
- inclusion, and participation
  - exclusion of people at the margins, and risk of perpetuating and exacerbating inequalities by not accounting for many different potential users (D2.4)

European values, laws, and ethical guidelines are identified in part from:
- human rights[23]
- human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities (see DEPS report[24])
- data minimisation and (de)centralisation (D2.4)
- https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

---

[23] https://www.europarl.europa.eu/factsheets/en/sheet/165/human-rights
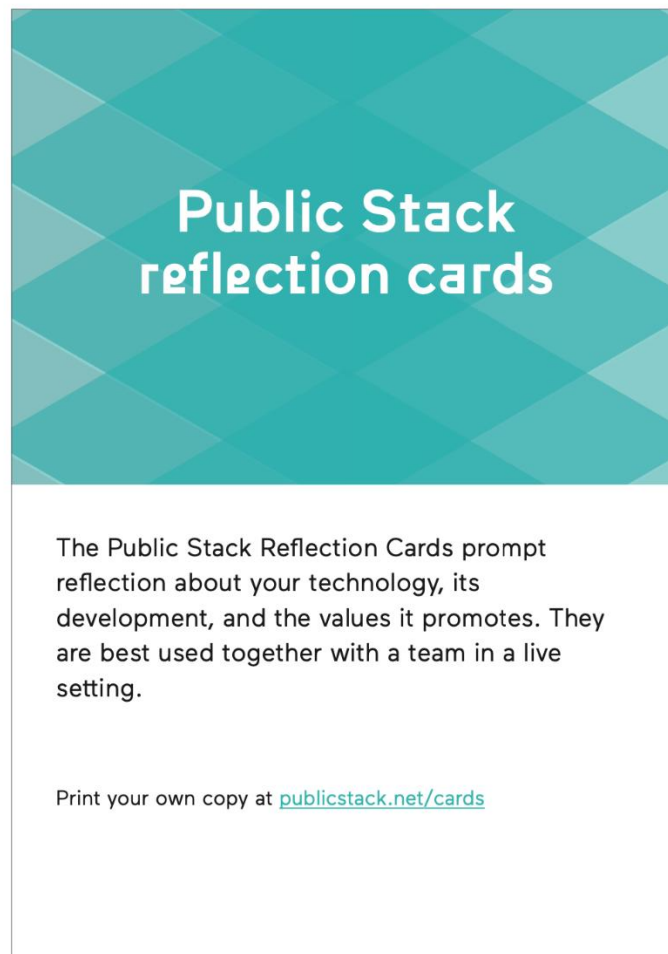[24] https://waag.org/sites/waag/files/2021-04/Waag%20Report%20on%20Digital%20European%20Public%20Spaces.pdf

- https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
- https://digital-strategy.ec.europa.eu/en/policies/digital-principles
- ownership and control over digital identity

7 Appendix II: Public Stack Reflection Exercise (Governance and Service Design Approach Tool – Cards)

For the print version, see https://publicstack.net/cards/

Public Stack
reflection cards

The Public Stack Reflection Cards prompt reflection about your technology, its development, and the values it promotes. They are best used together with a team in a live setting.

Print your own copy at publicstack.net/cards

What is the public stack?

The public stack is a way to uncover how the hidden layers behind technology relate to public values. You can take a public stack approach by:

→ identifying the public values in your project's **foundation**
→ facilitating an open and participatory **design process**
→ developing open source, fair, inclusive, and privacy-by-design **technology**
→ positively impacting **people & the planet**

Learn more at publicstack.net

How and when to use this?

Play, use, share or repurpose the cards however you see fit – whether at the beginning or during a development process that is already underway. In our experience it works best to discuss cards out loud as a team, with at least one other person present. Try documenting your answers as you go with sticky notes or a large canvas.

If this is your first experience with the public stack, we recommend starting out with the **foundation** cards.

Who made this?

ACROSS is a Horizon2020 public technology project funded by the European Commission under Grant Agreement 959157.
across-h2020.eu

Waag Futurelab contributes to the research, design and development of a sustainable, just society.
waag.org

public values

→ List the public values at the core of the project.

→ How are public values embedded in the project?

stakeholders

→ Who does this project belong to and who are the other stakeholders?

→ Who is affected by this project, but not directly involved?

starting points & assumptions

→ What problem does the project intend to solve?

→ When will the problem be solved? Who defines success?

governance & oversight I

→ What current mechanisms of governance are in place?

→ What resources and processes need to be governed in the project?

governance & oversight II

→ How can society monitor the project?

→ How is external (governmental or other) assessment ensured?

socio-economic considerations

→ How is the project financed? How does this impact the project?

→ Who might (economically, politically, socially) benefit from the project? At whose expense?

→ How is the technology maintained after its release?

open & participatory methods I

→ What methods are used in the project's development?

→ Is the design process participatory? Who facilitates co-creation? Who is included?

→ Which public values does the design process put into action? How?

open & participatory methods II

→ What mandate does the general public have to govern the design process?

→ How is transparency assured in the process?

→ Does the design process allow the project to change course based on feedback from the public?

users' journeys

→ Whose lived experiences are represented in the user journeys? Who is excluded or not represented in user journeys?

→ Who can and cannot use the technology?

→ Is the technology used in isolation, or as part of a group/community/network?

layers of technology I

→ What is the application, and is it in line with public values?

→ What is the operating system, and is it in line with public values?

→ What are the firmware and drivers, and are they in line with public values?

layers of technology II

→ What is the equipment, and is it in line with public values?

→ What is the infrastructure, and is it in line with public values?

→ Does the technology / product / service stand on its own or is it part of a larger ecosystem?

data I

→ What data passes through the technology?
With whom is it shared, why, and under what conditions?

→ What data is stored?
Where, why, and under what conditions?

→ When is data deleted? Do people have a right to be forgotten? How is this facilitated?

data II

→ Could the project potentially pose any threat to privacy or personal data control?

→ How is data sharing consent obtained and managed?

→ How does the project actively protect users' data?

data III

→ How do you encourage related, linked, and interdependent technologies to follow better (more secure, private, minimised) personal data practices?

→ Briefly sketch your data flow. How is this data flow in line with public values?
Where could it be improved, and how?

people I

→ How are 'end-users' positioned (e.g. as consumers, citizens, subjects)?

→ Are citizens enabled to advocate for their rights and interests in relation to this technology?

people II

→ How does the final product or service impact society?

→ How does the project merit public trust? How might it erode public trust?

planet

→ What is the project's environmental footprint?
What resources does it consume and require?
What resources does it protect?

→ Is the project in line with the Sustainable Development Goals?
Is it in line with local sustainability targets?

reflecting on the whole I

→ Where are the design process and technical layer in line with public values?

→ Where does the design process struggle (perhaps due to time, budget, context, or technical feasibility) to fully adhere to public values?

reflecting on the whole II

→ What are external impacts of the project (e.g. on the environment, nonusers)?

design dilemmas I

→ Where would you map the project on this continuum, and why?

open �⟶ closed

design dilemmas II

→ Where would you map the project on this continuum, and why?

anonymous users   identifiable users

design dilemmas III

→ Where would you map the project on this continuum, and why?

user control   automatic processes

design dilemmas IV

→ Where would you map the project on this continuum, and why?

decentralised   centralised