**A Digital Trust Infrastructure with embedded pulic values**Marije Kanis, Manon den Dunnen

Currently we are experiencing several challenges concerning personal data. Data is often collected without consent or with disguised consent, causing citizens and other data owners to lose control over (the use of) their personal data. This can negatively contribute to profiling (discrimination, exclusion) and cybercrime. Meanwhile it is laborious and complex for citizens and public institutions to obtain personal data in a transparent and responsible way. While at the same time, we see that a data-driven approach to social issues can also positively improve the quality of life, facilitate safety and innovation.
There is a need for a trusted infrastructure that, on the one hand, gives organizations and individuals control over their personal data and, on the other hand, guarantees the lawfulness, authenticity and safety of the personal data obtained. The aim of the Digital Trust Infrastructure (DVI) project is to jointly realize an independent public infrastructure for the conditional sharing of data. Public values ​​must be embedded in the infrastructure and the accompanying consent arrangement, so that the safety, freedom (autonomy) and privacy of those involved are guaranteed.

In order to define recommendations regarding desirable data exchange and public values, we (dr Marije Kanis of Digital life and Manon den Dunnen of the Police, and with the help of many professionals) have conducted a study into existing best practices for embedding and drafting these public values. In doing so, we came up with quite a list. We present the shortened version here, as an important shared lesson is to choose 2 - 4 overarching values that always apply. And then by determining for each case which values are specifically at stake, you can specify the concrete measures.

For the DVI we have identified the following overarching public values:

1. Control over data

Respect user’s autonomy and enable full control by the data subject, who can control, grant and withdraw their consent for the use of their data at any time. Data sharing should be based on user’s initiative and explicit consent and/or the law. Privacy by design is applied in every step of the design stage and throughout the life cycle. Conditions concerning large heterogeneous groups, like residents in our use case, will also be reviewed by expert representatives. This also includes the right NOT to participate; one should not be forced to share data, e.g. for full functionality or in return for getting help or other services. Therefore, we do not keep records of names for who does or does not participate.

2. Human-centered

This concerns both the participatory and user-oriented approach, as well as principles such as inclusion, contextual comprehensibility and accessibility. Fundamentally, it is about jointly solving a problem in a democratic way, by providing people with (1) a sufficient understanding of what is going on, and (2) the intellectual and practical tools to form an opinion and assessment of it, and where possible, (3) access to the technical tools to participate in it. Usage of the data sharing system should be rewarding to the data subject (first) and benefit other stakeholders like the firebrigade in our usecase as well.

3. Transparent

The workings of systems and processes are fully transparent and explainable to different target groups. In the event of problems, system processes and operations can be revised so that users can influence the workings. (Technical) complexity is limited as much as possible and is grouped in an orderly matter, so that there is a clear relationship between what people do and how it works technically (no magic in the background, no mixing of process levels). Different forms of data processing and data exchange are clearly distinguished from each other, and not one technical solution is used for all purposes, but an adequate solution is selected for every situation from a palette on which best practices have been agreed upon, and those best practices will be standardized when proven effective.

4. Trustworthy

This concerns availability, workability (for example, being able to act on time), correct operation (such as accurate, up-to-date data), robustness and security. True safety and security starts with people: how do they operate, what would a malicious actor do, how can users stay in control of their work, and make sure they and their systems are safe and not breached? Based on these questions only, possible solutions could be selected in the context of, for example, encryption and digital signing, but also to guarantee security and sustainability in general. Systems are accountable: open for checking its workings, (security) inspection, iiteration, mprovement, and to learn from. It is compatible with ethical norms and best practices recognized by the expert community.

By embedding these public values, including legislation and regulations, in the DTI, an independent, reusable, public provision is created. An attractive opportunity for anyone looking for cross-sector data sharing solutions, and who do not want to reinvent the wheel and make big investments!

The experiences and insights we have gained concerning public values and a participatory approach for the conditional sharing of data will soon be shared in a more elaborate report. So … stay tuned!