Brain-be 2.0
Belgian Research Action through Interdisciplinary Networks
POLICY BRIEF

Policy Brief n° 2

DIGI4FED- Digital (R)evolution in Belgian Federal Government: An Open Governance Ecosystem for Big Data, Artificial Intelligence, and Blockchain (DIGI4FED)

DIGI4FED aims to understand how (big) data can be used in the Belgian federal administration system to enable better public service provision through new technologies such as artificial intelligence and blockchain. By focusing on the technical, moral, legal and organisational conditions within the internal and external federal decision-making processes, DIGI4FED aims to develop a governance design that serves the administrative and public service processes of the Belgian federal government and makes full use of the potential offered by big data and its application via artificial intelligence and blockchain technology. DIGI4FED focuses on the development of a proof of concept (PoC) of a governance design – the design artefact – in two specific federal policy areas: social security infringements and tax frauds.

Project partners: KU Leuven, UAntwerpen, ULiège, UNamur
Project timing: 2020 – 2022

Context and question(s) of research

Three factors define the context by which DIGI4FED is influenced. The first factor is the growing attention to the potential impact of Big Data (BD) and Artificial Intelligence (AI) on traditional government information processes. The second factor is the growing expectation of society from public administrations, to adopt new technological means to advance efficient and effective governance and public service delivery whilst ensuring the core democratic and moral values are not lost out of sight. The third factor concerns the Belgian federal administration itself. Although several steps were taken toward the digital transformation of the Belgian federal state in the past, challenges remain.

DIGI4FED project has researched the conditions to introduce new digital technologies such as big data, AI, and blockchain to improve fraud detection processes in the taxation and social security domain. The ultimate aim of the DIGI4FED project is to outline a governance model of a data exchange platform that leverages open government data (OGD) and new digital technologies while complying with the specific requirements of the Belgian federal government ecosystem. Throughout the span of the project, the DIGI4FED team has gathered data through various means (e.g. experiments, interviews, living lab) to identify challenges to overcome in compliance with this aim. The details of the data collection and analysis processes have been reported in various deliverables (see D.1.3, D.1.4, D.2.2, D.2.3, D.3.2, D.3.3) produced as part of the project. To get a better insight into these processes, we invite the readers to check these deliverables.

Main findings

The research has revealed several types of challenges to the introduction of new digital technologies in the Belgian federal government. Below we highlight the key takeaways about how to address challenges in seven categorical areas: trust challenges, operational challenges, administrative challenges, technical challenges, user acceptance challenges, legal challenges, and policy challenges.

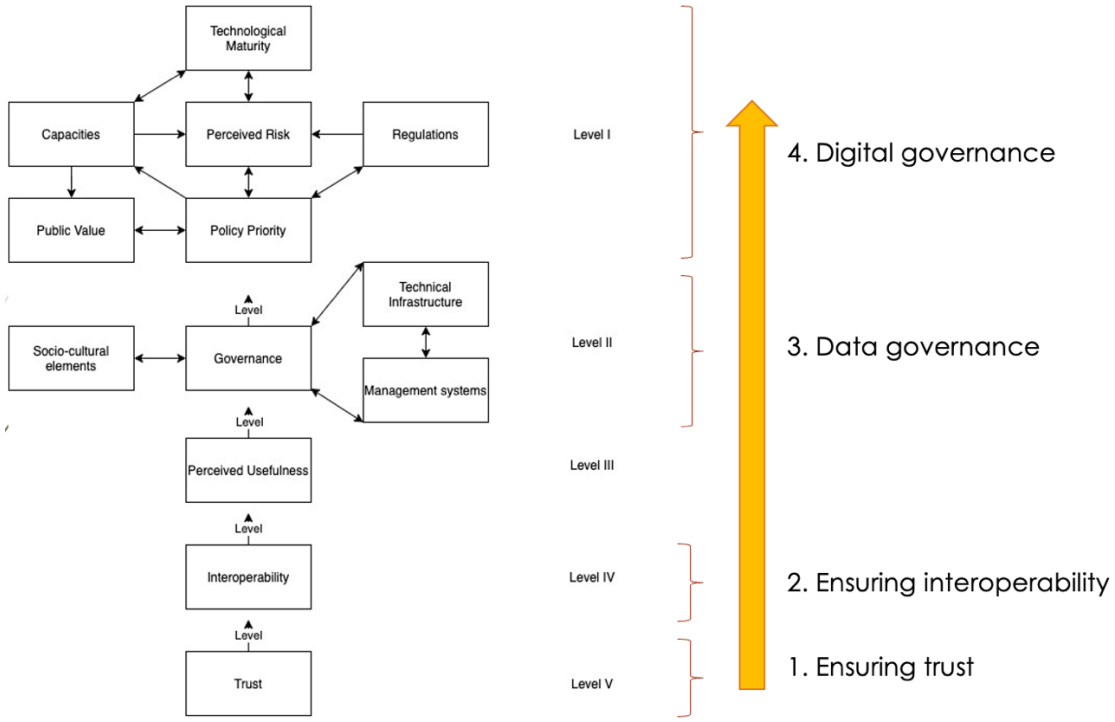
1. *Trust challenges:*
   - Transparency alone can sometimes reduce citizen trust in AI projects and data exchange platforms, in particular, if the information released may be perceived as threatening.
   - A combination of transparency and citizens' control over data maintain trust in AI project and data exchange platforms.
   - Citizens are willing to share data with the federal government but less so with commercial companies or regional and local governments.
   - Perceived discrimination is significantly related to trust in AI projects.
2. *Operational challenges:*
   - There is a lack of awareness across Belgian administrations about who holds what type of data in their databases. This hampers effective use of data in the fight against fraud and leads to waste of efforts and resources in competing projects.
   - There is a degree of lack of willingness to share data due to fear of administrative burden, and the absence of a long-term strategic and unifying vision to encourage data exchange.
   - The lack of common procedural and technical standards and the absence of a common platform that would ease data exchange between FPSs and outside organizations are hampering data exchanges to fight against fraud.
3. *Administrative challenges:*
   - Risks concerning access to sensitive data and the inability to control data service providers necessitate public sector organizations to lead the efforts in the governance of the data exchange platform.
   - But public sector organizations face disadvantages against private service providers in terms of mobilizing financial and human resources to support the governance of data exchange platforms.
   - Solutions developed by European actors and open-source solutions might reduce the dependence of the public sector on private sector organizations.
4. *Technical challenges:*
   - More advanced analytics solutions in the fight against fraud revoke concerns about explainability and fairness in decisions. XAI, decentralized technologies, and controlling the training datasets can provide solutions but the effectiveness of these solutions remain to be seen.
   - Fraud analytics with new digital technologies need to ensure a balance between explicability and effectiveness in fraud detection but a period of adaptation and learning would be necessary before adopting more advanced technological solutions
   - Investment decisions to centralized or decentralized technologies to support fraud analytics are closely related to public value, administrative, and policy challenges.
5. *User acceptance challenges:*
   - Governance design choices call for the assessment of public value implications.
   - There are counter-positions among the respondents about the purpose of a fraud detection system such as effectiveness vs. transparency, automated processes vs. human-controlled processes, and citizen-controlled processes vs. the only-for-once principle.
   - Usability and understandability are other challenges in design processes. The digital divide, technological self-efficacy of citizens, and regional differences in willingness to share data are important societal factors that can determine the success of technological solutions.
6. *Legal challenges:*
   - The current legislative framework on data processing rules limits the adaptability of advanced data analytics solutions in the fight against fraud. There are divergent interpretations by DPOs and difficulties in coordination and exchange between administrations.

- The legislative framework needs to be better aligned with the new digital technologies. However, how to achieve this alignment is debatable.
- Regulatory sandboxes and new EU initiatives and legislation on new digital technologies can be a solution, but clear guidelines and rules are needed for widespread adoption.

7. *Policy challenges:*
   - There are competing views on the desirability of decentralized and centralized systems solutions for the governance of the data exchange platform.
   - The data governance structure should address misalignments between different levels of government and pursue a unifying vision to facilitate coordination among European, federal, regional, and local initiatives in data exchanges.
   - The role of private actors in data governance needs to be clearly defined.

Conclusion and recommendations

The recommendations for building a governance model will follow the methodological steps identified by the interpretative structural model (ISM) presented in D.3.3. ISM explains the interrelationships among the drivers to implement new digital technologies in the fight against fraud in taxation and the social security domain. Accordingly, research findings are compiled into four areas of recommendation: (1) ensuring trust, (2) ensuring interoperability, (3) data governance, and (4) digital governance. Below we present the recommendations to establish a governance model that leverages advanced analytics in fraud detection.



Governance Issues	Policy recommendation
Trust	**Policy recommendation 1:** Pursue a transparent data exchange system that leverages self-sovereign identity (SSI) solutions and allows users to track data transactions
	Policy recommendation 2: Combine technological solutions with pedagogical / communication efforts toward citizens. But beware communication itself is not magic bullet.
Interoperability	**Policy recommendation 3:** Establish a single gateway to different departments, administrations, businesses, and stakeholder organizations to explore type of datasets held by different administrations.
	Policy recommendation 4: Create standardized documents and rules to facilitate data exchange through the single gateway.

	Policy recommendation 5: Integrate SSI solutions in the data exchange system in compliance with EBSI and ESSIF solutions.
Data Governance	**Policy recommendation 6:** Don't build a new data exchange platform to fight against fraud but address the system integration challenges among the relevant public and private organizations and existing data-sharing systems.
	Policy recommendation 7: Don't create a new entity to coordinate the data exchange for the fight against fraud. BOSA appears as the ideal candidate to coordinate other actors for the data exchange platform.
	Policy recommendation 8: Establish a data governance hub led by BOSA but participated by the representatives of regional and local government, as well as business and civil society organizations. needs to set the rules and guidelines in data extraction, sharing, and usage of platform data. A modular approach on data share and user rules is advisable.
	Policy recommendation 9: Manage data processing in the fight against fraud in a decentralized way, where data scientists are employed in respective units of social security and taxation domains but supported by the platform management in terms of legal and technical dimensions in data governance.
Digital Skills & Expertise	**Policy recommendation 10:** Collaborate with private sector organizations in developing technology solution in advanced analytics but pursue open-source technologies and build internal competencies in data analytics and advanced technologies to successfully engage with tech vendors.
	Policy recommendation 11: Invest in training programs and activities that supply advanced digital skills in public sector. Interdisciplinary trainings are necessary that combine computer skills with legal and social sciences dimensions.
	Policy recommendation 12: Provide frontline civil servants training and support to achieve a sufficient degree of data literacy and knowledge about advanced analytics. This training and policy support can be provided by the central management of the platform.
Value-based Design	**Policy recommendation 13:** Combine citizen-controlled data sharing (i.e. SSI) with transparency measures in data usage to maintain citizens' trust and engagement in digital governance.
	Policy recommendation 14: When suspecting that a particular data analytics tool may be perceived as illegitimate or discriminatory by some societal sub-groups, conduct research on how such a system would be interpreted by members of these sub-groups.
	Policy recommendation 15: Use legal, technical, and ethical requirements to design ethical procurement procedures for private sector service providers in advanced analytics.
	Policy recommendation 16: Engage in clear communication on the contents of digital change with end-users inside administration that are most affected by advanced techniques in fraud analytics. Avoid combining the integration of AI or data-driven support tools with excessive reductions in a specific category of frontline civil servants.
Policy Priorities	**Policy recommendation 17:** Make sure national and regional projects on SSI and digital wallets are compatible with EU-solutions.
	Policy recommendation 18: Participate in the EBSI use cases on taxation and social security to support the adoption of these solutions in the Belgian ecosystem.
Risk Management	**Policy recommendation 19:** Conduct in vitro-experiments to test the feasibility and understandability of XAI solutions for predictive analytics.
	Policy recommendation 20: Run controlled experiments to assess different technological configurations in data governance in finding a balance between performance of predictive analytics and understandability and transparency of algorithmic decisions.
Legal Compliance	**Policy recommendation 21:** Policy recommendation 21: Develop standardized guidelines for DPOs and DPA in managing open data policies for advanced analytics. IT solutions developed at the EU level have a clear advantage in facilitating DPOs' tasks
	Policy recommendation 22: Improve the reliability of IT solutions through regulatory sandboxes and benchmarking
	Policy recommendation 23: Pilot with regulatory sandboxes to test different regulative systems for the use of digital technologies in the fight against fraud.

Information

Contact
Tan, Evrim
KU Leuven Public Governance Institute
Evrim.tan@kuleuven.be

Crompvoets, Joep
KU Leuven Public Governance Institute
Joep.crompvoets@kuleuven.be

BRAIN-be 2.0*: BELSPO (the Public Planning Service Science Policy) organises a research programme designed to strengthen the scientific basis of federal public policy and the strategy and potential of the Federal Scientific Institutions (FSI) since 2012.*

More: www.belspo.be/brain-be