WHITE PAPER

The Ethics of A Platform for Data Sharing

This white paper addresses the ethical considerations around a new digital infrastrucure and social contract: The Data For Good platform for data sharing and individual data control.

November 2025

DATA for GOOD FOUNDATION

Index

Data for Care is an international consortium lead by **DATA For GOOD Foundation.** As a part of CRANE (EU-financed project) DATA For GOOD delivers together with international partners an ecosystem and a platform where personal data can be shared by citizens and used safely for self-empowerment and informed health policy decisions. The platform connects patients, health professionals and public health organisations together with digital service providers and researchers/analysts in new partnerships and digital ecosystems where data is shared and activated under the control of the citizen.

Executive Summary

This Ethics White Paper is developed as part of the EU-financed CRANE project, where Data for GOOD (DfG) provides the ecosystem and platform. The purpose is to explain how and why ethics are fundamental for DfG, analyse the model from an ethics perspective, and provide recommendations on how DfG can build trust.

DfG is about granting individuals digital sovereignty. It's about sharing of personal data (see more in Intro) in a trustworthy manner that empowers citizens and provides businesses and organisations with value derived from anonymised data.

Ethics is about doing the right thing; it goes beyond compliance with relevant laws and encompasses six core values: placing the human being at the centre, individual data control, transparency, accountability, equality, and sustainability. The 'BLTSEC governance model', developed by DfG serves as the framework for this report. BLTSEC stands for business, legal, tech, society, empowerment (and ethics), and communication and culture.

There is a growing demand for personal data - especially health and behavioral data - to advance treatment, prevention, and diagnosis, and for insights from anonymised personal data in research and analysis. Given Europe's strict personal data regulations, anonymised data represents a significant economic opportunity for the region. The key question is: whom will citizens prefer and trust when sharing their personal data?

The Data for Good Foundation (DfG) acts as a trusted third-party data intermediary, operating on behalf of individuals and governed by strict European laws and a robust governance model. DfG ensures that individuals can give informed consent for the use of their data - whether anonymised or not.

Business. DfG can adopt several of five described business model, though not without risks. Charging service providers and organisations an onboarding fee and an annual license is reasonable as long as they are aligned with DfG's Manifesto. Charging for anonymised insights is also fair, provided there is consent, but this approach carries risk, as many citizens struggle to distinguish between identifiable and anonymised data. When it comes to partners, sponsors, and subcontractors, it is crucial to clearly communicate why DfG collaborates with companies, be it big tech or other commercial companies, emphasising that these partnerships offer users more advantages (such as greater control and new insights) than disadvantages.

Legal. Legality in data practices means adhering to national and EU laws, which directly shapes public trust. While companies like Meta historically used opt-out models or forced consent to maximize data collection, the EU advocates for explicit opt-in consent, ensuring users actively engage with and understand data usage terms. The Data for Good (DfG) platform embraces this opt-in approach, aligning with GDPR's privacy-by-design principle and prioritizing transparency and user trust. DfG's Crane project meets all legal requirements.

Tech. To build trust in technology, Data for Good (DfG) relies on Partisia's cutting-edge, open-source platform, which integrates secure multiparty computation, encryption, anonymization, blockchain, and privacy-by-design. This technology enables collaborative data processing without exposing raw data, and ensuring privacy and security. Key benefits include calculations on encrypted data, data quality stamps for reliability, tamper-proof logs, and benchmarking against anonymized datasets, all without transferring or duplicating data. Ethical risks are de-anonymization attempts, user journey bugs, over-reliance on Partisia, and inconsistent use of non-EU tools.

Society. As a neutral, non-profit foundation, DfG is legally required to reinvest surpluses into society and faces dissolution if it strays from its mission, with mandatory annual transparency reports ensuring accountability. By adopting a non-profit structure and open APIs, DfG fosters interoperability, and attracts commercial partners seeking to demonstrate societal impact. In a world where health data is often locked in closed platforms, DfG champions individuals' rights to access, share, and benefit from anonymized data, enabling new insights and advancing a fair, sustainable data economy for all.

Empowerment. While the DfG platform empowers citizens, the most obvious initial target groups are those who need to use their data, such as patients, and sports enthusiasts. Empowering individuals is fundamental to a democratic society, but it should not include the ability to sell personal data, and digitally illiterate users will need extra focus.

Communication & Culture. The communication challenge is huge, as success depends on a shift in digital culture, from convenience to self-empowerment and responsibility. Ethical communication must be clear, genuine, transparent, and constructive, avoiding exaggerated or unrealistic promises. The recent emphasis on digital sovereignty, particularly in the wake of Trump's second term, has helped ease this challenge.

In a nutshell, DfG grants Europe an ideal platform for a data democracy where individuals - not the state nor big tech - are controlling their own digital lives. The challenge is that there are no big buyers.

To be a success, the European politicians and authorities must embrace platforms like DfG. If they want their data regulation to live up to their visions of a human-centered data democracy, they should start walking the talk and lead the way to citizens' control of their own data.

Recommendations

⟶ DfG should develop a clear ethical framework, the DfG Manifesto, outlining the principles for all partners, service providers, sponsors, staff, and subcontractors, who must formally commit to its standards.

⟶ When individuals obtain data control via the DfG platform, they can donate their data anonymously. To begin with, it should only be for charitable purposes. Any sales of anonymised data with consent should initially be trialled through pilot schemes to gauge user reactions.

⟶ DfG should emphasise that users can reclaim their data from big tech and other companies or the public sector, and could provide clear, step-by-step guidance on how users can retrieve their data from big tech services.

⟶ DfG must be transparent about pricing structures and ensure there are robust safeguards against the risk of de-anonymisation, as outlined in the DfG Manifesto.

⟶ To avoid over-reliance, DfG should collaborate with a broader range of technology providers beyond Partisia, and diversify on service providers, too.

⟶ It should be made clear that users can (or will be able to) withdraw their data from the platform and exercise their right to data portability.

⟶ Pilot schemes have revealed several issues in the user journey, which may deter users from adopting the solution. As the technology matures, these problems are expected to be resolved upon full implementation.

⟶ DfG and its partners should transition away from Google Suite, opting instead for European alternatives such as Nextcloud or Proton Docs.

⟶ DfG should politically advocate for the individual's right to combine data from multiple sources and for the fact that the Data Governance Act is eased so it can better act on the commercial market.

⟶ The DfG platform should discourage users from selling their own data.

⟶ It is crucial to engage influential figures and decision-makers to promote the potential of self-empowerment through data.

⟶ DfG should continue targeting groups with a pressing need for data utilisation, such as sports enthusiasts and patients, as well as the privacy-conscious elite who recognise the value of their data. Partnering with organisations to encourage group participation is a way forward.

⟶ In the long run, DfG must find a way to focus on how to include more vulnerable, non-digitally literrate patients in the ecosystem to ensure equality.

RECOMMENDATIONS to policy advisers and the public sector

⟶ The current rules in the EU make it hard for a data intermediary to operate in a commercial market. Therefore, policymakers should ease the requirements of the Data Governance Act so that a data intermediary can generate revenue on sales of anonymised data and insights to cover its costs.

⟶ Both policymakers and the public sector, in general, should demonstrate much more courage when it comes to acting on digital sovereignty and speaking out against both the Chinese and US data models.

⟶ The public sector in the EU should be first movers when it comes to using European technology and empowering citizens with control over their own data. Walk the talk.

Intro

From the citizens' point of view, the digital world is an expensive and complicated affair. Not only must we pay for an increasing number of services with money, but we also pay, at an unknown but likely high cost, with our personal data. We are not in control of our own data, nor our digital lives; others are.

There are three main models for data control. The first is the US model, where big tech and commercial interests are in the driver's seat when using of personal data. The second is the Chinese model, where the government maintains control. In both, citizens have no authority over their own data. Europe, by contrast, aims for a democratic, value-based approach. In practice, however, the reality is a mix of all three models, depending on how privatised or state-governed a country is.

In Europe, laws place the individual at the centre, giving them control over their data. With the GDPR, the Data Governance Act, the European Health Data Space, and the Data Act, citizens and consumers theoretically have the power to manage their data. The GDPR grants the right to data portability, allowing individuals to request their data in a usable format from any service, while the Data Act strengthens this right. The Data Governance Act (DGA) regulates intermediaries that facilitate secure data sharing between individuals and other parties.

Yet, in reality, most people never exercise these rights. Many are unaware they even have them, and even if they are, they often don't know how or why they should use their data. The digital market lacks services that help individuals leverage their data for personal or societal benefit. We know that data can empower people and that anonymised data can drive societal and economic progress, but the potential remains largely untapped.

The vision of The Data for GOOD Foundation (DfG) is to foster a democratic society built on honesty and trust, where citizens are in control over their own data, and data is used responsibly to create value for the common good.

The DfG sees itself very much in line with an interview study from Fraunhofer-Institut für Software- und Systemtechnik ISST that looks at the expectations placed on data

intermediaries. That it is human centric in its architecture, uses state-of-the art technology for secure data sharing, that it promotes data sovereignty, is a regulations navigator, provides an ecosystem for data sharing, and satisfies the needs of all suppliers in the value chain. See enclosure 1.

The purpose of this ethics white paper is to:

- Explain why ethics are fundamental to Data for GOOD (DfG) and CRANE, identifying and clarifying the core principles;
- Analyse the DfG governance model from an ethical perspective;
- Provide specific recommendations on how DfG can build trust through an ethical approach.

If we examine the intent behind Europe's laws and regulations, we might describe Europe's ambition as a data democracy, a model distinct from a data dictatorship (as seen in China) or a data monopoly (as in the US). In a data democracy, where the individual is at the centre, there is significant potential, especially at a time when mistrust is growing rapidly. This is further compounded by geopolitical shifts, where the US is no longer seen as a natural ally, reigniting Europe-wide discussions on **digital sovereignty**. The imperative is clear: Europe must take control of its own digital infrastructure, including its data.

Trustworthiness has become a critical currency. It demands genuine transparency, delivers real value, and empowers individuals, just as in any democracy, with self-agency, whether in their real or digital lives. Amid the global surge of misinformation, AI-generated falsehoods, and the misuse of personal data by both governments and private companies, DfG tries to put trustworthiness into the sharing and use of personal data.

Ownership and control of one's own data are essential to sustaining a democratic foundation in today's knowledge-driven society.

The former city manager of Aarhus states in Kommunen[1]

This paper focuses on **personal data**, with specific focus on health data and behavioural data, a central priority for both DfG and CRANE. Personal data encompasses two key categories: Data collected, analysed, and stored by national healthcare systems during

[1] *https://www.kommunen.dk/artikel/personlige-data-kan-give-livreddende-foerstehjaelp-til-skrantende-sundhedssektor*

patient treatment. And data gathered by citizens themselves through an expanding market of devices measuring everything from steps and pulse to temperature, blood pressure, and sleep patterns. This creates a complex data landscape. Personal data is governed by diverse national laws, often inconsistent across countries, as well as the overarching GDPR. As a result, data is fragmented across multiple silos, some state-controlled, others commercially managed. The legal framework is intricate, and ethical considerations add another layer of complexity.

There are two primary uses for personal data when it comes to our health; **Primary use:** Supporting treatment, prevention, and diagnosis, including decision-making tools for both citizens (empowerment) and healthcare professionals. **Secondary use:** Enabling research and analysis, such as the development of new medicines, medical devices, evidence-based treatments, and innovative therapies.

What Is Ethics

In 2022, a researcher from the Capital Region of Denmark's psychiatric services obtained approval to access hospital records for 3.65 million Danes, covering data collected from 2000 to 2030. This is likely the largest research project based on medical records ever undertaken in Denmark. Through the Precision Psychiatry Initiative, the research team aims to use AI to analyse vast datasets, exploring the causes and effects of mental illness and developing computer models to assist doctors in assessing psychiatric patients.

When the project was publicised[2] in September 2025, it sparked significant debate:

- While the research purpose is legitimate, individuals should still have the right to opt out.
- The public must be informed about how their data is being used.
- People have a right to know who is accessing their data, for what purpose, and how it will be used.
- Such practices erode trust and may deter patients from seeking help from public healthcare services.
- The combination of health data and AI carries a higher risk of misuse.

Beyond the fact that the Capital Region failed to conduct a Data Protection Impact Assessment (DPIA) before releasing the data (an oversight now under investigation by the Danish Data Protection Authorityt[3]), it appears no laws were broken. For years, Danish researchers have enjoyed privileged access to pseudonymised or anonymised personal data for scientific purposes without requiring individual consent.

Legality is one matter. Ethics, particularly regarding trust, is another. Today, even when using fully anonymised data, it can be argued that individuals should be asked for permission. Without it, people may perceive the use of their data as an abuse of trust. What if their data contributes to developing treatments they personally oppose? While financial compensation may not be the issue, transparency and consent often are.

---

[2] *https://www.dr.dk/nyheder/indland/forsker-har-faaet-lov-bruge-millioner-af-danskeres-sygehusjournaler-uden-de-ved-det*

[3] *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/datatilsynet-indleder-undersoegelse-af-region-hovedstaden*

This example highlights the ethical dilemmas surrounding the secondary use of health data, which often raises more concerns than primary use, where data is applied directly to patient treatment. In contrast, Data for Care (as decribed in a box on page 2) also focus on primary use, demonstrating how the Data for Good platform can support digital health services.

Ethics is about confidence and trustworthiness. It means doing the right thing with respect for the individual citizen. It is about handling personal data in the same way you would want your own daughter's personal data to be treated.

This report is grounded in six core principles of AI and data ethics (see Enclosure 2), drawn from the EU High-Level Expert Group on Trustworthy AI[4] and DataEthics.eu:

The human being at the centre
Individual data control
Transparency
Accountability
Equality
Sustainability

These principles serve as the foundation for every chapter of this report, which is structured according to the governance model developed by the Data for Good Foundation, BLTSEC (see Enclosure 3). By adopting this approach, we aim to demonstrate how ethics can be practically implemented and operationalised.

[4] *https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai*

B for Business

To promote individual data control, a viable business model must be in place to sustain the DfG platform economically. Companies and organisations need to see clear economic value in collaborating with DfG. For a business to be considered ethical, core ethical principles must apply, which DfG upholds: human benefit takes precedence over profit, and individual data control is central. Full transparency in business operations is essential, as is accountability in decisions about partnerships.

VisitData is a national Danish platform that provides the tourism sector with new insights to optimise competitiveness. It relies on combining anonymised data, including summer house and camping bookings, retail turnover, event calendars, mobile data, weather data, and indexed spending etc. When analysed and combined this data reveals valuable patterns — for example:

Forecast guest on the island of Bornholm *Tourism data is used to forecast number of visitors and guests weekly using both historical season data, regional vacation calendars and actual ferry bookings, looking one, two, three and four weeks ahead. With AI, we calculate a forecasted number of additional and total bookings within a given period – this with very low margin of error; 3.5% in worst case and below 1.0% in the best cases.*
Optimizing business on Rømø *Numerous data sources to gain insight into the tourist behaviour, movement and buying on the island of Rømø were used to predict staff planning and evaluation of capacity in cafés like Fru Dax. In addition, these insights were used to open another café as numbers showed that Café Dax were not enough to serve everyone.*
Road work at Hvide Sande *In order to plan maintenance of key roads for, data from holiday home rentals was used to show when there are few guests and tourists in the area of Hvide Sande in order to cause the least possible traffic inconveniences for locals, business and tourists.*

Developed by the global Japanese firm NTT DATA Business Solutions A/S, VisitData inspired one of its managers to consider: *"What if we did the same with health and behavioral data?"*

The Data for Good Platform provides an ideal framework for extracting value from personal data. Collaborations on the platform can generate value in two key ways:

1. Digital services, where citizens 'data is transformed into personalised insights, creating value for both the individual and the company, whether through customer acquisition and retention, improved operational efficiency, or risk prevention.

2. Analysis and research, which delivers value to researchers and businesses by uncovering new insights.

Through DfG, companies, organisations, and other stakeholders can request consent to use anonymised data. DfG can carry out confidential computing analyses. These analyses use encrypted personal data from services and applications within the platform's ecosystem. Calculations are performed via multiparty computation, producing aggregated insights and statistics without exposing raw data.

There is undoubtedly a substantial demand for insights derived from anonymised personal data, whether for research, treatment, or societal benefit, as well as for profit and growth. Given Europe's strict data protection regulations, this approach represents a significant economic opportunity for the continent.

The EU Health Data Spaces also aim to maximise the use of anonymised data, but a critical question remains: Will citizens and consumers trust companies or governments to handle their personal data responsibly? Might they instead prefer a trusted third party, e.g. a data intermediary acting on their behalf, governed by strict laws such as the Data Governance Act and a secure governance model (see 'S 'for Society) to manage their consent for data use, whether anonymised or not?

This is precisely what DfG offers in this implementation phase of its platform via the Crane projects (see page 2). While DfG operates under a non-profit governance model, it still requires revenue to sustain its ecosystem. The challenge, then, is: What business model would users find acceptable while maintaining trustworthiness?

Business Models of an Intermediary

DfG has not yet applied to become an official data intermediary under the Data Governance Act due to its stringent requirements (see the section on 'Ethical Business Risks'). An intermediary acting on behalf of citizens must have a sustainable revenue model and cannot rely solely on public or private grants.

Below are the five primary revenue-generating options, followed by an ethical analysis of each.

Five Potential Revenue Models

1. **Sales of anonymised insights.** The foundation will sell anonymised insights, but only with explicit user consent each time. Users receive indirect value, such as greater control over their data and access to empowering services, including personalised insights.

2. **Revenue-sharing of sales of anonymised insights with users - via tokens.** Users earn tokens each time they share their data. Revenue is distributed between the users, partners, the foundation and may be a charity of the user).

3. **Subscription, license, and fees.** DfG will charge organisations and service providers onboarding fees, annual licenses, and pay-per-use fee pay for insights, ananlysis and research depending on number of users, data sources, frequency, complexity etc.

4. **Sponsorships and donations.** Revenue will be generated through corporate sponsorships and philanthropic donations.

5. **Membership fees.** Income will be derived from individuals, companies, or organisations paying membership fees to access the platform.

DfG's planned business model (as illustrated in Enclosure 4) combines especially option 1, 3, and 4. Below, each of the five models is analysed for its ethical implications.

Re. 1. **Sales of anonymised insights.** This model is ethically sound, but it must be introduced gradually to help users understand their powerful role, particularly the importance of active consent for each transaction. There is a fundamental difference between selling anonymised insights with explicit consent and the historical practices of

big tech, which have profiled users and sold access to their data, often without consent. Given this context, users may remain skeptical about any form of data monetisation. To build trust, I recommend that initially, data should only be donated anonymously for ethical or charitable purposes, with pilot projects introduced later to gauge user reactions to the sale of anonymised insights.

DfG will need to establish a clear ethical framework (e.g., the DfG Manifesto, as outlined in the Conclusion) to define acceptable partners. And also, it will have to maintain full transparency regarding pricing and data usage.

Re 2. **Revenue-sharing of sales of anonymised insights with users - via tokens.** While the idea of users earning money from their data may seem appealing, revenue-sharing introduces an ethical dilemma: It risks positioning DfG as a facilitator of data sales, which is problematic. Data is deeply personal - akin to a person's organs - and even when managed through a regulated intermediary, its commercialisation remains ethically questionable. DfG should not enable or encourage individuals to sell their data, as this undermines the core principle of data sovereignty and could erode trust in the platform.

DfG cannot and should not prevent individuals from choosing what to do with their own data. If users wish to sell their data, that is their prerogative. However, DfG has a responsibility to inform users about the potential benefits and risks of such actions.
For instance; It may be acceptable for an insurance company to offer discounts to members of a sports club. It is a practice already seen in Germany and potentially elsewhere in Europe. What is unacceptable, however, is tying insurance discounts to daily step counts, a model employed by some US and UK insurers, which crosses ethical boundaries by incentivising invasive data collection.

Re 3. **Subscription, licenses and fees.** Onboarding fees and annual licences represent a clean and ethically sound business model. However, all customers must adhere to the DfG Manifesto, ensuring alignment with the platform's ethical standards. If added with sales of anonymous insights as in 1, it carries the same ethical risks as in 1 and should be introduced cautiously,

Re 4. **Sponsorships and Donations.** Both are suitable revenue models for an intermediary. However, it is critical to define strict criteria for which sponsors are acceptable. Displaying logos from data-broking companies would undermine public trust in DfG. In contrast, partnerships with ethically aligned brands could be permissible, as these companies are not

data brokers. A clear ethical framework, such as the DfG Manifesto, is essential to guide sponsorship decisions. It is also important to note that DfG's commitment to donating any surplus to charitable causes falls under its governance model, not its business model.

Re. 5. **Membership Fees.** Membership fees are another strong and ethically sound revenue model, as income is distributed across a broad base of individuals and organisations. This approach minimises the risk of DfG being associated with controversial data brokers. Membership should be open to all, whether individuals or organisations, based in Europe or elsewhere. A tiered fee structure could be implemented, with different rates for individuals and organisations. It is however, questionnable if enough individuals will pay for individual data control services. All members should be required to sign the DfG Manifesto, ensuring alignment with the platform's ethical principles.

Ethical Business Risks

Data for Good Foundation faces several ethical business risks that could impact its mission and credibility:

Disengaged Citizens
Over the past two decades, digital citizens and consumers have grown accustomed to convenience, easy-to-use, and 'free' services (where the real cost is their data). Many automatically accept terms and conditions without reading them, and some have given up on controlling their data and digital lives. Even if DfG offers a platform for individual data control, many may not engage, regardless of the opportunity.

A Continuous Restrictive Data Governance Act (DGA)
The EU's Data Governance Act (DGA) imposes strict rules on certified data intermediaries, emphasising neutrality and non-exploitation of data. The primary business opportunity for DfG lies in facilitating data transactions, not direct monetisation, even of anonymised data, as discussed earlier. If the DGA remains unchanged and DfG wants to be a certified data intermediary, it could lose the ability to sell anonymised insights. However, reports from EU insiders suggest that some relaxation of these rules may be possible.

Ethical Risks in Partner, Sponsor, and Subcontractor Selection
DfG's choice of partners, sponsors, and subcontractors carries significant ethical risks. For example; Fitbit (owned by Google/Alphabet) is currently used by DfG, despite Alphabet's history of data exploitation. While users can export their data from Fitbit/Google, thus

exercising their GDPR right to portability, this does not eliminate the risk of association with Google, which could damage DfG's credibility.

Some partners to DfG also rely on Microsoft Azure or Google Cloud Storage, which may be legally and politically acceptable but ethically questionable, especially when European alternatives are available.

Mitigating Ethical Business Risks

To address these risks, DfG can take the following steps:

- Focus on target groups most likely to engage, such as athletes or patients.
- Partner with organisations to encourage group participation, for example, enabling sports clubs or patient groups to donate self-collected data such as sleep patterns to scientific projects or personalised health tools. It will be far more effective to engage larger groups with shared goals than to convince individuals one by one.
- Collaborate with organisations like MyData.org and Fraunhofer-Institut für Software- und Systemtechnik ISST to advocate for adjustments to the DGA, particularly regarding how intermediaries can generate revenue ethically.
- Clearly communicate why DfG works with commercial companies, emphasising the benefits for users (e.g., greater control, new insights) over the drawbacks. Highlight that DfG enables users to reclaim their data from big tech and others to empower themselves and society.
- Diversify service providers (e.g., Apple Watch, Garmin, Oura Ring) to avoid indirectly promoting any single brand like Fitbit.
- Provide clear, step-by-step guidance on how users can retrieve their data from big tech services.
- Require partners, sponsors, and subcontractors to commit to phasing out non-European cloud services by signing the DfG Manifesto.

L for Legal

Legality is about complying with national and European laws. Legality directly influences whether citizens and society trust a solution. Given the varied interpretations of these laws, it is crucial for DfG to be clear and transparent about its legal framework and to uphold the spirit of the law, not just its letter.

For years, users have grown accustomed to opting out of data practices they oppose, ticking 'No' to unwanted data collection. However, Meta took a different approach in 2018 when the GDPR came into force. Instead of offering an opt-out, Meta rewrote its terms and conditions, making it impossible to use Facebook without indirectly consenting to profiling and behavioural marketing. Six years later, in 2024, the European Data Protection Board (EDPB) ruled this practice illegal, stating that Meta must obtain explicit opt-in consent from users for tracking and targeted advertising. As of November 2025, a legally accepted solution is still pending.

Big tech prefers opt-out models (or no choice) because they know most users won't read the terms, let alone actively opt out. The EU, however, advocates for opt-in solutions, as they encourage users to engage with the terms, understand the implications, and make an informed choice. If users do not opt in, their data should not be tracked by default. This approach aligns with privacy-by-design, a core principle of the GDPR. While enforcement has been slow, opt-in is increasingly seen as an ethical necessity rather than just a legal requirement.

The DfG solution is built on an explicit opt-in model, fully aligned with the intentions of the GDPR. While big tech and some digital designers dismiss opt-in as an obstruction, it is the only ethical path forward if we want confident, engaged users. DfG delivers a transparent, user-centric approach that prioritises consent and trust.

Every time a user's data is required for a purpose on the DfG platform, an explicit opt-in and consent are requested. To enhance convenience for the user, the platform could offer varied consent options. For example, users might choose to grant a one-year consent for European university researchers to use their data, while preferring to provide separate consent each time their data is sold anonymously to private companies.

Consent, encompassing understanding, context, and transparency, is particularly critical when discussing AI in healthcare. The Danish Data Ethics Council has examined the use of AI in this field and emphasises:[5]

"There is no general requirement for consent regarding the use of AI healthcare. Nevertheless, considerations regarding consent and self-determination for patients and healthcare professionals are important. AI technologies rarely appear as a separate choice, but rather as an integrated or upgraded technology in already known elements of a treatment. Consent in the context of AI is therefore not just a matter of yes or no, but of understanding, context, and transparency."

The DfG platform is the natural choice when AI is applied in healthcare, whether for direct patient treatment or research purposes.

From a legal standpoint, the Crane project by the Data for Good Foundation complies with all requirements, supported by a legal white paper, a data flow analysis, a Data Protection Impact Assessment (DPIA), a data management plan, and data processing agreements with every participant in the ecosystem.

While data ethics and law share common goals, as both aim for responsible data and technology use, they differ in focus. Law establishes the regulatory framework and rules governing data processing, whereas ethics addresses the moral principles and values that should guide how data is handled. Therefore, being legally compliant does not automatically ensure ethical practice, though it is an essential foundation for it.

[5] *https://dataetiskraad.dk/Media/638859134124585016/Ansvarlig%20AI%20i%20sundheds-%20og%20velfrdsteknologier_Dataetiske%20perspektiver.pdf*

T for Tech

For trust in any technology to be established, multiple criteria must be met, not just in the governance model (see 'S' for Society) or the business model (see 'B' for Business), but especially in the technology itself. In the case of DfG, this means cutting-edge, state-of-the-art technology.

The platform's technology is developed by Partisia, a global encryption company originating from Aarhus University. It incorporates open-source technology, secure multiparty computation, encryption, anonymisation, blockchain, and privacy-by-design.

At its core, Partisia enables multiparty computation, a method that allows multiple parties to collaborate on computing tasks without revealing each other's underlying data. While all parties receive the results of the computation, no single party gains insight into the others' data. This ensures data privacy, security, and responsible governance, particularly critical in the health sector.

The technology is blockchain-based, with key components of the platform being open-source. The protocols used for calculations and the platform itself are open-source, though the user-facing apps operate under a licence model.

The advantages of this technology are as follows:

- Enables calculations to be performed directly on encrypted data, ensuring privacy and security are maintained throughout the process.
- Can assign data quality stamps, ensuring that medical data from healthcare professionals is prioritised over less reliable sources, such as fitness trackers.
- Creates a detailed, tamper-proof log of all data interactions, proving that data has not been altered and ensuring it is used only for its intended purpose.
- No data transfer or duplication is required. The platform connects data sources without moving them, leaving the original data holder responsible for keeping information up to date.
- Allows organisations or individuals to benchmark their own data against aggregated, anonymised datasets without ever exposing raw data from other users.

While the DfG platform leverages cutting-edge technology, several ethical risks must be addressed:

- Although de-anonymisation attempts are not illegal, they can be ethically unacceptable. To mitigate this risk, stronger safeguards could be implemented, and a commitment to prevent de-anonymisation should be included in the DfG Manifesto, requiring all partners and subcontractors to adhere.
- Pilot programmes have revealed several bugs in the user journey, which could undermine trust in the platform. As the technology continues to evolve and mature, these issues are expected to be resolved.
- Currently, Partisia is the primary technology provider. To reduce dependency risks, DfG should expand partnerships to include alternative providers, such as the digital wallet iGrant or the Solid pod, ensuring greater flexibility and resilience.
- It must be explicitly clear that users can (or will be able to) export their data from the platform, fully exercising their right to data portability under the GDPR.
- There is an ethical inconsistency in DfG and Partisia staff using Google Suite, despite the availability of European alternatives like Nextcloud or Proton Docs. This undermines the platform's commitment to data sovereignty and should be addressed.

On a positive note, Partisia hosts its data with Hetzner, a German cloud provider, demonstrating a commitment to European data infrastructure and reducing reliance on non-EU services. This is a best practice that aligns with DfG's ethical and legal principles.

S for Society

It is essential to examine ethics not only from the perspectives of individuals or businesses, but also from a broader societal viewpoint. The DfG's governance model is structured in a way that is strictly regulated by Danish law, leaving no option to change its purpose.

WhatsApp, launched in 2009 by two Ukrainian-Americans, was once considered as secure and private as Signal is today. However, after its acquisition by Facebook in 2014, its reputation for privacy and security declined significantly. This highlights a major risk; an organisation with strong ethical principles can be sold to a company with conflicting values, compromising user trust. To mitigate this risk, some privacy-focused services now guarantee users that, if acquired, they can retrieve and delete their data before ownership transfers. Or they pledge never to be sold at all.

The Crane platform from Data for Good Foundation (DfG) follows the latter approach. DfG is established as a neutral enterprise foundation with a charitable purpose, ensuring that any surplus is reinvested into society. It is rooted in Danish fund legislation and operates as a neutral data intermediary.

A foundation cannot change its purpose, and if a foundation operates against its purpose it will be closed by the authorities. Therefore, it cannot convert into a for-profit company nor be acquired. It would have to shut down entirely and restart under a new structure. Annual statutory reports on foundation principles are mandatory, ensuring transparency and credibility. This is the same legislation that governs trusted entities like the Novo Nordisk Foundation.

DfG has added an extra layer of trust by adopting a non-profit model, similar to Signal. This ensures that any surplus is donated to projects aligned with its mission, further reinforcing its commitment to societal benefit.

"The purpose of the Data For Good Foundation is to champion awareness, dissemination, and use of database-driven development, health promotion, prevention, and disease treatment to contribute to development, growth, and public health locally, nationally, and globally."

As a non-profit organisation, DfG appeals to commercial partners, as it can give them a touch of 'changing society for the better' reputation. Collaboration with DfG offers companies the opportunity to demonstrate their commitment to positive change.

DfG further distinguishes itself by aiming to use open APIs, fostering interoperability and technological independence. Recognised by the MyData Organisation for its governance and thought leadership, DfG builds trust among citizens and consumers, encouraging them to share their data with confidence.

Today, most health-related data is collected outside the healthcare system and beyond users' control, often locked within closed platforms such as those of Google and Apple. As DfG believes that individuals, communities, and society should have the right to access, share, and benefit from anonymised personal data, it is supporting a fair and sustainable data economy for all. DfG is a key advocate and enabler of the right for individuals to combine data from different sources, gaining new insights to improve their lives and contribute to the greater good.

E for Empowerment

Many digital health services are about giving the citizen more responsibility over their health, treatment, and rehabilitation. In this empowerment of the citizen, ethics are vital if the users should trust a service with their data. But the empowerment should not include the possibility of selling data.

A Danish diabetic patient has taken control of his own treatment and is empowering himself with his data. With hundreds of data points a day, he can keep his diabetes regulation at the level of non-diabetics, he says. Blood sugar, data from his insulin pump, his intake of carbohydrates, his steps, and other activity data, plus his quality of sleep are all processed inside his own homemade app, which gives him a prediction of his insulin needs. If his Oura ring tells him that he slept badly, he usually needs 10% more insulin. He is comfortable with a blood sugar level around five, but that does not really work with the values set by traditional pumps. With his own system, he experiences fewer blood sugar spikes and more stable blood sugar levels, which are necessary for diabetic patients to live a good life.

Other diabetes patients are doing the same. They hack their own regulations, you could say, but commercial apps for diabetics are slowly catching up and offering to combine blood sugar levels with weight and activity data. This idea of empowering individuals with their data is very good, but most informed patients would most probably trust their data with a neutral intermediary rather than a commercial service. And therefore, the idea of empowerment should align with the vision of DfG.

The most obvious target group for empowerment includes people with a need to use their data, and that is patients and sports enthusiasts. Many already use their data for better treatment or performance, but most people could benefit from their own data, whether they are dog walkers or couch potatoes. And being involved means more engagement.

"When professionals and patients are involved as partners in the process – and not just as end users, both the professional quality and legitimacy of the solution are strengthened. It also increases the likelihood that the technology will be used responsibly, because those with practical experience can contribute their knowledge, needs, and perspectives early in the development process. At the same time, involvement can help to increase the sense of ownership and self-determination, both for healthcare professionals and patients, and ensure that AI is used in a way that is in line with both professional and personal values."

These are the words of the Danish Data Ethics Council recommending[6] that data should be used to empower patients.

Ethical risks

One thing is the empowerment of the individual to access their own data to improve their life or contribute to society. Another matter is how the individual might otherwise use their data as a sales object.

In Denmark today, it is fully legal to analyse other people's data without seeking permission, provided the data is anonymised and, for example, obtained via Statistics Denmark. As discussed in the chapter What is Ethics?, seeking permission is the ethical approach. Most citizens would consent to their data being used in scientific research if they feel in control and trust the researchers. But how far would they go if they could actually earn money by selling their data?

From a societal perspective, allowing a market for the sale of personal data to flourish is not ethical. The greatest risk here is human behaviour: if individuals get the opportunity to sell their own data, and do so through the DfG platform, they might take it, even though the price for individual data will always be low.

Another ethical risk is leaving out the most vulnerable, those who are not digitally literate enough to participate and take control of their own data. The Crane project is focusing on users in rural areas and on getting everybody onboard, but the pilots are pretty narrow. Therefore, as the DfG platform grows, it is essential to focus on involving the most vulnerable groups, who might need extra education or even counselling.

[6] *https://dataetiskraad.dk/Media/638859134124585016/Ansvarlig%20AI%20i%20sundheds-%20og%20velfrdsteknologier_Dataetiske%20perspektiver.pdf*

C for Communication & Culture

There is a fine line between communication and marketing. Many commercial tech companies tend to exaggerate, even lie about the potential of their services. Ethical communication is clear, genuine, transparent, and constructive. Communication of individual data control goes hand-in-hand with culture. A huge cultural change regarding the control of personal data is a prerequisite for effective communication.

A decade ago, the founder of the Data for Good Foundation, Annemette Broch, first spoke about her vision of individual data control at a conference organised by DataEthics.eu in the heart of Copenhagen. Around the same time, the Finnish NGO MyData.org was launched with support from the Finnish Ministry of Transport. Over the past decade, the EU has written and implemented laws to give individuals the right to their own data (see L for Legal). Many start-ups have launched, trying to help individuals control their own data, and some have given up.

The communication challenge is huge because it depends on a change in digital culture. It is about implementing this European third way, where the citizen, not the state or companies, is in control of their own data.

Part of the challenge is big tech, which offers convenient, easy-to-use services where you 'just 'pay with your personal data (and time, because you help train it) and often do not understand the risks and societal consequences of being dependent on a few gigantic companies with different values and views on democracy. Many digital users have become suckers for convenience. Furthermore, governments in Europe, despite having made laws in favour of individual data control, often want to be in control of as much data as possible themselves.

So, to succeed, communication and culture need to go hand-in-hand. European governments and companies must show their willingness and courage to let individuals be in the driver's seat of their digital lives. DfG needs services that demonstrate what this means, and the communication challenges will become more tangible and perceptible.

With the new focus on digital sovereignty following the Trump era, the communication challenge has been eased slightly, as the idea of using European tech has become common

sense to many. Yet, the challenges remain massive in light of the money spent on soft power by big tech[7] to continue selling their services in Europe.

The right strategy is to target large organisational partners who have members they can activate to take control of their data. However, those members, individuals, will need incentives and convenience to bother giving active consent and activating their data.

Just like the green movement, it is about getting started and targeting the most well-educated and digitally literate, and, of course, those who really need their data: people who suffer from chronic illnesses and athletes. The majority will not find it interesting to take control of their data before there are enough services, showing that it is worthwhile and attractive.

It is important to find role models and people in power to promote the possibilities of self-empowerment through data and the insights that can be gained from anonymous data.

And finally, a huge company or public organisation will have to show courage and join the platform wholeheartedly. Then the snowball will start rolling, and the education process for citizens and consumers can truly begin.

[7] *https://dataethics.eu/softpower/*

Conclusion

The DfG eco-system puts ethics at the center of all six parts in the BLTSEC-model, and is an example of innovation in agreement with democratic values and regulation, opposed to many claims that regulation hinders innovation.

Business. DfG ensures that *human beings are at the centre*, so they benefit before profit. *Individual data control* is a core purpose. Chosing between the proposed business models, ethical frameworks, *transparency*, and user trust can be obtained. Sales of anonymised insights should start with charitable donations to build trust, while revenue-sharing via tokens risks ethical concerns by commodifying personal data. Subscriptions and licenses are ethically sound if aligned with DfG's principles and all parties sign up to the DfG Manifesto. Sponsorships must be selective to avoid associations with data brokers, and membership fees offer a broad-based, ethical revenue stream, though individual uptake may be limited. The main risk to address is that the vast majority of individuals may not bother to take control of their own data.

Legal. The DfG solution is an explicit opt-in model and thus designed in full accordance with the intentions of the GDPR, namely, opt-in. This demonstrates *accountability*. Legally, the Crane project by the Data for Good Foundation complies with all relevant regulations, which is a prerequisite for upholding data ethics.

Technology. The system uses secure, proven, state-of-the-art encryption, making it possible to perform calculations on encrypted data, benchmark an individual's data against anonymised patterns, and keep data at its original source. This technology truly delivers *individual data control*. However, DfG needs to address the risk of de-anonymisation, bugs in the user journey, and the need to include more tech providers. Portability issues must be clear, and DfG's use of services outside Europe should be replaced by European alternatives.

Society. The DfG governance model puts *human beings at the centre* and is structured in a way that is strictly regulated by Danish society. It is altruistic and addresses *sustainability* in the meaning of social concerns, as any surplus is returned to society.
However, the risk is that society may not 'pay back 'and support a model like DfG, as some public sectors want to retain control of data rather than empower individuals with more control and responsibility.

Empowerment. Empowering citizens by giving *them individual data control* also places more responsibility on them. Therefore, it is a good idea to start with citizens most likely to be interested in what data can do for them, namely, patients and athletes. It's likely that the most digitally literate will be the first obvious users; therefore, DfG must focus on *equality* by ensuring that the most vulnerable patients are not left behind. This is done with education and ease of use.

Communication & Culture. Ethical communication is clear, genuine, *transparent*, explainable, and constructive, avoiding exaggerated or unrealistic promises. Communication of individual data control goes hand-in-hand with culture, as a huge cultural change regarding the control of personal data is a prerequisite for effective communication. If his cultural change - such as a major player like the public sector taking the lead - is not initiated, the communication challenge may be too great.

Where is the Demand?

The DfG platform is, in a nutshell, the perfect platform for a data democracy where individuals control their own data for the empowerment of themselves and the benefit for the welfare society.

All three pilots seem to want to implement a platform like DfG for their citizens, but they are waiting for more services and users. And here is the catch-22. As one interviewee said: *'It is a deeply honourable project. But it is also a kind of pseudo-project. There are no buyers.'*

Another interviewee said*: 'The challenge is that if there is no political support for allowing citizens to control their own data, then it may not matter. As a public authority, we might even feel greater ownership of data than the citizens themselves. So, that political clarification is still missing.'*

Another public servant said about the DfG platform and its values: *'I simply don't see another way.'*

For DfG to succeed, the public sector in Europe must take the first step, lead the way, and embrace a platform like DfG. Today, most of Europe still uses - and thus promotes - services from the US, despite the existence of perfectly viable European alternatives[8].

If European politicians want their visions for the past decade's new data laws to be realised, they should start walking the talk and lead the way to citizens 'control of their own data. The DfG platform has been in development for 10 years. It is more than ready, and EU funds have given it the final push towards implementation. It is time for full commitment from the political side.

The DfG Manifesto & Ethical Oversight Board

An ethical framework - a DfG Manifesto - is necessary when signing up to the DfG eco-system and when hiring staff for the foundation. This first draft for a DfG Manifesto should be finalized with inspiration from other manifestos such as The Sutainable Software Manifesto[9], and thus be signed by all customers, subcontractors/partners, sponsors, staff, and organisational members of DfG.

1. We live up to relevant law, and will comply with the guidelines when updated by the Ethical Oversight Board.
2. We will put citizens first and make sure they and possibly the society benefit from data processing before profit or efficiency gains.
3. We believe in individual autonomy and empowerment and in individual consent to the use of personal data - anonymised or not.
4. We are transparent about pricing and our data process, and we explain when asked.
5. We believe firmly in privacy and equality.
6. We care about the environment and act accordingly.
7. We will strive towards using open source and/or European services, and promise to try and move away from big tech services asap.
8. We will work towards individual data control by helping citizens take back control of their data, and we will be inclusive.
9. We will not try to de-anonymise data.
10. We will not help individuals sell their own data.

[8] *https://dataethics.eu/tools/*

[9] *https://sustainablemanifesto.org/*

As ethical challenges pop up continuously, it is a good idea to set up an independent Ethical Oversight Board and feed it with ethical challenges on the go. It should consist of experts from both the public and private sector, from Denmark, the Nordics, and internationally, and it should meet 2-3 times a year (online or in person) to discuss ethical issues.

End Note

This report is based on field research and in-depth interviews with relevant sources with knowledge of DfG/Crane, data intermediaries, and European data regulation. The author has followed and reported on - both as a journalist - the movement advocating for individual data control since 2011. https://fonts.google.com/specimen/Rubik

About the author

Pernille Tranberg has been in the advisory board of Crane in phase 1 and 2 and is the author of this whitepaper in phase 3 of Crane. She is an independent speaker, analyst, and advisor in data democracy, and data- and AI ethics.

She is the co-founder of the European think-do-tank DataEthics.eu, and she was appointed by the Danish Ministry of Business to be part of the expert group on big tech between 2022-2024. She has followed the MyData movement since it's inauguration in 2010-2011 and DfG since 2016.

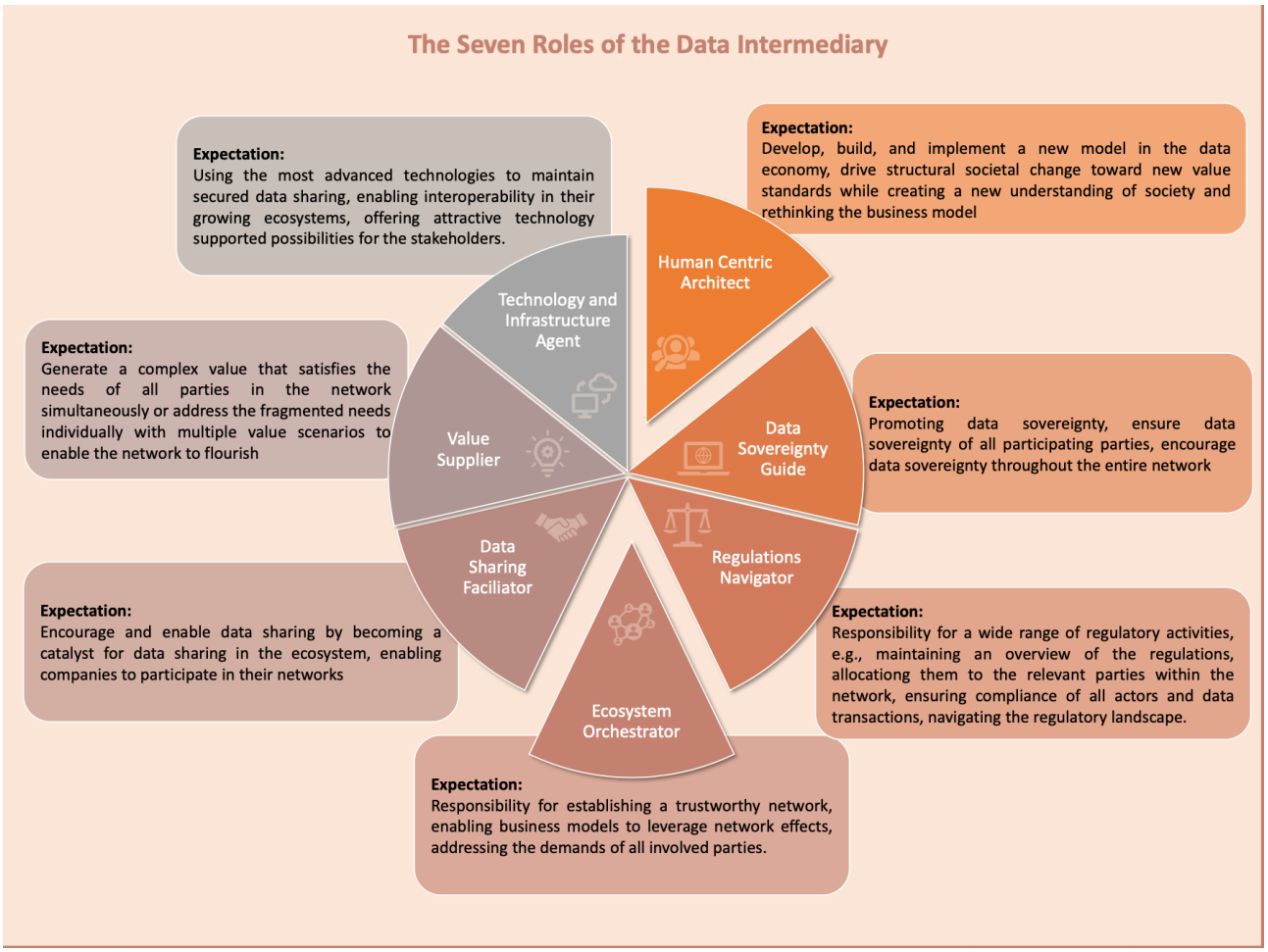
She is a journalist and former tech and investigative reporter, editor-in-chief, and head of editorial development at leading media outlets in Denmark. She holds a Master's Degree in Journalism from Columbia University, New York (1995) and has written 8 books: the latest is 'A Data Democracy Comes With Individual Data Control '(2021), and 'DataEthics – The new Competitive Advantage '(2016) with Gry Hasselbalch. She co-authored 'Fake It '(2012, Peoples Press) about big data and digital self-defense, and the report 'Big Tech Soft Power'.

Frontpage illustration: Generated by the European chatbot Le Chat - chat.mistral.ai

Enclosures

Enclosure 1

First eveluations for an interview study on 'Business Models of Data Intermediaries' by Fraunhofer-Institut für Software- und Systemtechnik ISST, November 2025. After looking at the expectations placed on data intermediaries, the institute plans to formulate and then formulate a business model that meets these expectations.



Enclosure 2

THE HUMAN BEING AT THE CENTRE
Human interests always prevail against institutional and commercial interests. People are not computer processes or pieces of software, but unique with empathy, self-determination, unpredictability, intuition, and creativity, and therefore have a higher status than machines. The human being is at the centre and has the primary benefit of data processing.

INDIVIDUAL DATA CONTROL
Humans should be in control of their data and empowered by their data. A person's self-determination should be prioritised in all data processes, and the person should be actively involved in the data recorded about them. The individual has the primary control over the usage of their data, the context in which his/her data is processed, and how it is activated.

TRANSPARENCY
Data processing activities and automated decisions must make sense for the individual. They must be truly transparent and explainable. The purpose and interests of data processing must be clearly understood by the individual in terms of understanding risks, as well as social, ethical, and societal consequences. (opt-in)

ACCOUNTABILITY
Accountability is an organisation's reflective, reasonable, and systematic use and protection of personal data. Accountability is an integral part of all aspects of data processing, and efforts are being made to reduce the risks for the individual and to mitigate social and ethical implications. An organisation's accountability should also apply to subcontractor's and partners 'processing of data.

EQUALITY
Democratic data processing is based on an awareness of the societal power relations that data systems sustain, reproduce, or create. When processing data, special attention should be paid to vulnerable people, who are particularly vulnerable to profiling that may adversely affect their self-determination and control or expose them to discrimination or stigmatisation, for example, due to their financial, social, or health related conditions. Paying attention to vulnerable people also involves working actively to reduce bias in the development of self-learning algorithms.

SUSTAINABILITY

Preventing harm and ensuring fairness are core aspects of sustainable personal data processing. Sustainability addresses both environmental and social concerns with the goal of benefitting all human beings, including future generations. To achieve this, the two concerns should be seen as intertwined. Thus, by tackling a pressing social need by processing data in an environmentally friendly way, the process and its outcome is sustainable.

Enclosure 3

The Governance Model is rooted in an ideal vision of creating a public good based on a promise to citizens of individual data control and a fundamental need to secure trust between the users and stakeholders across the eco-system. The core components tying the ecosystem together are the DfG platform and Governance model. Compliance to EU data regulation is genuinely incorporated as a core service into the DfG platform and based on the 3 key features; DfG single sign-on, consent management and personal data store. Security, privacy and anonymity is possible due to the MPC Technology running a network of nodes governed by DfG, that ensures the organisation can achieve valuable insights without compromising privacy and sharing sensitive information.

To secure trust from citizens towards sharing their data with the eco-system, governance must take a holistic approach. This is why DfG with inspiration from MyData.org have developed the BLTSEC = TRUST model - 'DfG Good Governance', where a carefully selected number of concrete principles, demands and actions under each of the five themes below together aims at promoting and maximising trust in the platform and eco-system as a whole.

- B = Business - e.g. transparency, accountability
- L = Legal - e.g. compliance, data management
- T = Technology - e.g. state-of-the-art, proven
- S = Society - e.g. neutrality, interoperability
- E = Ethical - e.g. data ethical framework and principles
- C= Communication & culture

The 'Good Governance model' includes clear agreements between the stakeholders within the eco-system and with the customers on roles and responsibilities, ie. regarding onboarding, education and communication, support and maintenance.

Enclosure 4

The planned business model of DATA For GOOD Foundation.