EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

Media and Data
Unit G.1 – Data Policy and Innovation

An emerging offer of "personal information management services"

Current state of service offers and challenges

1. INTRODUCTION

In July 2014, the Commission adopted Communication (COM(2014)442 on a thriving data-driven economy. In this communication it announced to "launch a consultation process on the concept of user-controlled cloud-based technologies for storage and use of personal data ("personal data spaces")".

In this document we report on relevant findings collected by DG CONNECT. It contains in particular:

- Results from a public online consultation on the question whether personal information management is perceived as an interesting way forward for a wider public;
- A detailed description of the current service offerings in the area of personal information management in Europe, including technological and commercial readiness of the service offerings;
- A description of future R & I challenges and other potential areas of public (and EC) intervention.

This document was finalised in January 2016.

2. DEFINING THE THEMATIC SCOPE

Evolution in technology allows handing back control over use of personal information into the hands of the individual concerned. A number of initiatives have developed over the course of the past 5 years with the aim of providing platforms and/or services to individuals in view of handing back such control.
While considerable conceptual variations exist, the vision is to work towards the following:

- A control function (e.g. console or dashboard provided via a web page or app) allowing the individual to define access to and usage of the data at a highly granular level in terms of which data (or sub-sets of data) can be accessed, by whom and for what purpose and foresee also the option to withdraw consent at

Commission européenne, 2920 Luxembourg, LUXEMBOURG - Tel. +352 43011
Office: EUFO 1177A - Tel. direct line +352 4301-31613

malte.beyer-katzenberger@ec.europa.eu

any moment (concept of "dynamic consent"); such definition should be assisted by a manageable, predefined set of options for access and use;

- outside parties wishing to use data can access and use the data in conformity with the expressed preferences through secure exchange protocols for requesting and exchanging personal information; in the alternative, outside parties can either bring their computing algorithm to the data on the platform (never seeing the actual data) or procure insights on the basis of an "analytics-as-a-service" offer;
- incentivise use of such platforms by offering an added value to the individual in the form of services and applications, thus going beyond a mere "data vault or locker". This exploits the fact that in an ideal scenario any individual's personal information management platform aggregates data from a variety of sources, making it an ideal place for data integration at the individual level, enabling the development of a who new class of "personal (Big) data" applications.

The term "data spaces" chosen in COM(2014)442 suggests the preference for storage of the data in a dedicated "data vault" or "locker". Some initiatives, however, do not foresee such central storage. Also, the consultation process showed that there are projects/initiatives that do offer slightly different services or services that currently do not offer the full service as described in the vision above. Consequently, the broader term "personal information management services" (PIMS), also employed outside, is used here.

3. THE EVIDENCE-COLLECTION PROCESS

The evidence-collection process consisted of three elements:

- a questionnaire sent to known initiatives/ companies providing or developing personal information management services and related actors in Europe;
- a round-table discussion with these initiatives/ companies and related actors that took place on 27 November 2015;
- two questions in the public online consultation on the "Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy".

Replies were received from the following organisations:
a) Solution providers and similar:
Mydex, Meeco, digi.me, healthbank Cooperative, MiData Cooperative, Qiy Foundation, Forgerock, the Hub-of-all-things, Danube Tech, TISEI, OpenConsent, CozyCloud, Synergetics, the openPDS project, Data Mixer, Telefonica, Telecom Italia, Peercraft, University of Cambridge (Data Box), MyWave and Coelition.
b) Organisations supporting the evolution of personal information management services:
Fing, Helsinki Institute of Information Technology, Ctrl+Shift, Lynkeus, Alexandra Institute and UK Digital Catapult.
c) Public authorities:
Romania and Sunderland City Council.

Member States and organisations participating at round-table meeting on 27 November 2015 without written statements:
Slovak Republic, Estonia, INRIA TAO, Digital Me, CapGemini NL.

Member States and organisations contacted without reply or participation at the meeting of 27 November 2015:
Finland, KMD, Glome, Orange Telecom, Pidder, Paoga,

4. FINDINGS

4.1. An emerging issue for a wider public?

The public online consultation on platforms, intermediaries, data and cloud and the collaborative economy running in autumn 2015 allowed the Commission to test the opinions of an open public.

Two questions were asked in respect to personal information management services:

- Do you think that technical innovations, such as personal data spaces, should be promoted to improve transparency in compliance with the current and future EU data protection legal framework? Such innovations can take the form of 'personal data cloud spaces' or trusted frameworks and are often referred to as 'personal data banks/stores/vaults'?
- Would you be in favour of supporting an initiative considering and promoting the development of personal data management systems at EU level?

55% of the respondents to the section of the public online consultation on "Data and Cloud" responded to the first question[1]. 53% of these respondents said that personal information management solutions should be promoted (185 responses). 30% responded negatively and 17% said that they had no opinion.

On the second question, only 28% of respondents answered the question (176 actual replies). Out of these respondents, 90% replied in the affirmative (158 respondents).

We note the difference of 27 respondents who are generally in favour of "personal data spaces" but do not see the need for EU intervention.

When analysing the numbers, one needs to be aware of the fact that a large number of other questions in the same section have seen "no response" rates of 40-50%, meaning that the number of respondents to the first question is overall in line with response rates for this section of the survey.

Overall, the replies to the public online consultation show that there is some sensitivity of a wider public to the issue of personal information management. Given the fact that this

[1] 351 actual responses to the first question, out of 635 respondents who answered questions in the section on "Data and Cloud" and 1005 responses that were collected in the public online consultation overall.

emerging sector is known only to very limited audiences, only very preliminary conclusions can be drawn from this consultation.

4.2. The landscape of offerings and related actors

In Europe, 20 organisations are active in the field of developing some kind of platform or service enhancing privacy protection in the online world.

16 initiatives[2] have as objective the developing some sort of technical platform that is designed to enable the individual to access and control usage made of his/her personal data. Among these, 3 initiatives[3] focus on health-related information. The others aim at taking care of any **kind of data**.

The remaining 4 initiatives focus on the consumer-brand interrelationship[4] and on consent-as-a-service[5].

In terms of **geographic spread**, there is a strong representation of UK organisations (6), whereas the others are from Austria, Belgium, Denmark, France, the Netherlands, Spain, Switzerland. Two initiatives from the US (openPDS, Forgerock) and two from Australia (Meeco, MyWave) were accepted as they have already or aim at establishing a customer base in Europe.

Researchers at Helsinki Institute of Technology, Fondation Internet Nouvelle Génération, the UK Digital Catapult, INRIA TAO (FR), Alexandra Institute (DK) as well as the specialised UK-based consultancy Ctrl+Shift are following the evolution of the sector and/or are contributing to individual research challenges.

Out of the 20 initiatives, almost all organisations developing the platform architectures are small in **size**: 6 declared a company staff level to be between 1 and 10; another 8 are between 10 and 50. Only 1 is above 100. 5 respondents did not answer this question. This gives an indication that scaling the platforms to large user audiences is a major challenge for most initiatives.

We have identified a small number of larger organisations that experiment with personal information management, namely Telecom Italia and Telefonica. Deutsche Telekom and Orange appear also to prepare some form of personal information management service, but have not communicated any details.

We observe also that many of the actors surveyed are not operating in pure isolation, but build trans-national alliances, applying together for funding, filling gaps in the technology of their platform.

---

[2] Mydex, Meeco, digi.me, healthbank Cooperative, MiData Cooperative, Qiy Foundation, Forgerock, the Hub-of-all-things, Danube Tech, CozyCloud, Synergetics, the openPDS project, Data Mixer, MyWave, Data Box, Model-driven digital repository (presented by Lynkeus).

[3] healthbank Cooperative, MiData Cooperative, Model-driven digital repository (presented by Lynkeus).

[4] TISEI, Peercraft, and Coelition.

[5] OpenConsent.

4.3. Commercial readiness

6 initiatives[6] are currently offering personal information management services and are reporting expanding their offers in terms of "corporate" clients. 4 initiatives[7] are announcing revenue service in the first half of 2016. The remainder have not indicated specific dates for launch of revenue service or have not answered the question.

Mydex offers a personal data store that allows individuals to collect organise and distribute data about them, their lives and the world around them. The collection of verified attributes and subsequent sharing of them can reduce effort and friction in online transactions and increase trust and confidence and enable seamless transactions to completed online either via web or API interface. Additionally, a privacy-friendly portable identity called a MydexID allows individuals to login anywhere that open standards are supported and access services without creating a new username and password. A consent and permissions management utility that allows individuals track where, when and with whom who they have shared their data and for what purposes. A set of utilities that allows them to collect and organise data from their own line activity e.g. address books, bookmarks, browsing history, location data, credentials and social network activity.

MyWave proposes an entirely novel way of vendor relationship management offering frictionless end-to-end outcomes for companies and individuals. Leaping potentially into the digital future, it uses a personal information management service to allow companies to pro-actively contact the individual on his/her smart device through a personal assistance tool with truly relevant, "hyper-personalised" offers, anticipating needs on the basis of information provided and on the basis of the consent of the individual. It is currently offered in Australia and New Zealand. Commercial activities in the UK are foreseen to begin in spring 2016.

Digi.me offers to the service to download locally (and subsequently synchronise) data uploaded onto social networks back into a data store on the basis of a desktop application, using the right to data access and the APIs of the relevant networks. Current functionalities are limited to some analytics for personal use. Opening up the digi.me to allow businesses to contact individuals is planned for 2016. Digi.me is active internationally, reaching out to important actors in several domains.

[6] Mydex, Meeco, digi.me, Coelition, MyWave, Forgerock, MyWave and Synergetics

[7] CozyCloud, OpenConsent, TISEI, Model-driven digital repository (presented by Lynkeus), healthbank Cooperative

Meeco is a privacy-enabling life-management platform offering an app for mobile devices with a view of integrating invidual data to the maximum extent possible. It is a zero-knowledge platform, meaning it has no access to the data held. It offers an encrypted data vault and the ability to exchange data based on permissions as well as to signal intents for products or services so that the providers of such products or services can approach the individual. Additional features include applications to analyse data ('quantified self'), private messaging and a private web portal.

The Qiy Foundation is an independent trust organization. It created a scheme, principles, and a model for a human-centric approach to the managing and processing of personal data. The Qiy Scheme has been operational since January 2015. What's new is the fact that people can be part of the digital network, having their own terms and conditions exchanging data. Certified parties can implement an infrastructure which serves as the engine enabling a secure control over personal data. Currently, three services based on the Qiy Scheme are in operation:

- Dappre is the interoperable and networked version of the old business card idea, making it digital and intelligent Through Dappre, individuals can subscribe to each other's information. Companies can subscribe to (validated) data of its customers. Apart from self-declared information, Dappre facilitates connections with validated information with a digital signature, validated and certified by human resource departments, compliance officers and/or external providers.. Whenever an individual or an organisation changes their data, all others who have subscribed to this information will receive notifications of these changes and -in turn- can act upon these changes and update their own systems (if needed).
- The town of Boxtel has started to establish trust relationships with their citizens on the basis of the Qiy Scheme.
- Verzeker uzelf is an online insurance broker that has started to use the Qiy Scheme for the creation of trust relations with its customers.
- A future use application under development is a webshop which interacts with (potential) customers without having to know anything else than what has been ordered and that the order was paid for: https://relying-party.was4.digital-me.nl/relying-party/

Box: Examples of personal information management services currently on the market

The challenge of identifying a sustainable business model:

Personal information management services are facing the challenge of getting multi-sided platforms[8] to the market characterised mainly by:

- The culture of the provision of "free" services for individuals over the internet, making it unlikely that a sufficient number of individuals will agree to pay for personal information management services;
- The difficulty of winning over data-holding organisations as they have invested heavily to reach the capacity to collect user data and consequently have no natural interest to broaden access to such data, including by through personal information management platforms;

As any new market entrants they face the challenge to earn the trust of individuals and companies alike. The privacy-friendly business promise will not – by itself – create the necessary trust. Some respondents fear that – in an optimal scenario where there is important uptake on personal information management platforms – there will be a "gold rush" and also less trustworthy actors will offer such platforms. There is a risk that a lot of emerging trust in personal information management services in general will be destroyed by a small number of "black sheep" in the market.

Business models are currently being experimented with take different forms:

(1) Organisations intending to run a personal information management platform:

They tackle the challenge of getting multi-sided platforms to the market by experimenting with approaching the multiple sides (mainly: individuals, data-holding companies, developers of applications using the data put on the platform) simultaneously using most often "hybrid" models:

- Freemium models are being applied vis-à-vis individuals (free use of basic functionalities, additional functionalities, e.g. individual analytics on top of data offered by the platform against payment)[9];
- Companies may be asked to pay a transaction fee for consumption of data from the platform[10]; this can take the form of bulk provision of (anonymised) data or interactions with individual users in exchange for monetary or other rewards;
- Apps developers share part of revenue from app sales with platform (similar to other "app stores");
- Some platforms think about offering analytics-as-a-service on top of the data and fund the platform partly on this basis[11]; this could represent in itself a privacy-preserving design facilitating Big Data analytics on top of personal information.

[8] Platforms creating value by enabling direct interactions between different distinct types of customers, creating benefits from network effects;
[9] This is part of the current business model of Mydex, Meeco, digi.me.
[10] It goes without saying in this context that such consumption needs to be based on the individual's consent.

(2) Personal information management as platform-as-a-service[12]

Personal information management platforms can also be provided to specific companies or organisation striving to improve either their service offer to the end clients (personal information management as an additional service) or aiming at improving their vendor-client relationship through a privacy-friendly means of interaction. Governmental actors[13] can likewise be clients when exploring personal information management in order to allow citizens to better manage access to and use of their data in an "eGovernment" context, e.g. in a setting where the "once-only" principle[14] is applied. Revenue in this context is generated by fees on the organisation using the platform.

Network effects are to be expected by any of the three sides (individuals, data input coming large corporate actors and applications on top of the data) growing in numbers.

Respondents suggest that **companies** will be willing to pay transaction fees for trusted interactions with individuals as personal information management platforms will enable **access to better quality data** to a **wider audience of actors**, with the technical possibility to obtain consent or to improve their trust relationship with customers. Corporations will see efficiencies in peer-to-peer interaction, notably on their advertisement efforts, given the rise of ad blockers and the increasing market dominance of certain platforms. Consumers being less and less receptive to traditional advertising also will expect entirely new forms on outreach, where personal information management platforms can be instrumental. Also, they will see lower compliance costs (notably with the future General Data Protection Regulation) and increased customer engagement. They will be willing to pass on a part of the savings made in this context to the individual and the platform.

Additionally, personal information management platforms capable of offering enable **micro-payments** directly to the individual in exchange for data use on the basis of consent, provide an additional trigger to sign up for such platforms.

The two examples of healthbank Cooperative and MiData Cooperative follow the cooperative model under which the individuals wishing to use the platform are becoming members of the underlying legal entity ('the cooperative') and are required to buy a membership share feeding into the capital base of the organisation. Additionally, healthcare institutions seeking to share medical data of their patients through the healthbank Cooperative platform will be asked to pay a fee. MiData Cooperative

[11] This is the core feature of OpenPDS' SafeAnswers mechanism and also contemplated by Synergetics.
[12] This model is e.g. offered or contemplated by Forgerock, CozyCloud,
[13] Notably UK local government bodies, but also some Member States such as the Netherlands, the Slovak Republic or Romania.
[14] This refers to the principle that citizens should be requested by government to only submit any given information or document only once in a setting where governmental authorities are then requested to share the information or document. It may appear desirable to foresee the storage of such information in a PIMS platform and allow the citizen to only authorise the access by another authority upon specific request, avoiding the unnecessary free circulation of documents or information among just any governmental authority.

specifically excludes any monetary compensation to individuals for use of their data by third parties for ethical reasons.

The ethical dimension of emerging business models

The business models (present and future) need to be assessed also against an ethical dimension.

If some of the effects of using personal information (unsolicited advertisement and similar, price discrimination in the context of sales over the internet, other forms of discrimination or refusal of service and similar) can be regarded as negative externalities of processing of personal information, the user cannot be asked to pay for enhanced privacy. Privacy also cannot be subject of a cost barrier, reserving it to the richer parts of the population only.

This would argue for organisations processing personal information to pay for privacy-preserving personal information management. This approach can take two forms: Having the platforms paid through fees by the companies who originally collected the personal data (personal information management services as part of the compliance obligations of such companies) or by third parties who would like to access such data for other purposes (either directly from the individual or purchasing access in bulk and/ or in anonymous form).

Making such third parties pay for personal information management platforms (or hybrid models) will, however, result in a **conflict of interest** for the provider of the personal information management platform, in particular under the first approach (platforms having individuals as their direct customers). The platforms will need to incentivise the individual to store and to share as much information about him/herself in the platform as possible, possibly more than the individual would have wanted, so as to generate the necessary revenue.

In that respect, models according to which personal information management platforms are part of a wider service offer (online bank account, internet service provision or other) appear favourable.

What remains of utmost importance is to ensure the **transparency of the business model** vis-à-vis the end customer.

A realistic view on the further evolution and roll-out on personal information management systems

Citing the example of the relative failure of the Respect Network's ambitious plans[15], some of the respondents took the view that at this moment of the evolution of the market for personal information management solutions there is a need to concentrate efforts on tackling individual areas rather than aim for an encompassing ecosystem. Such areas

[15] One respondent deeply involved in the Respect Network development attributes the relative failure of this approach to the overly ambitious approach of building a huge, encompassing ecosystem.

could be improving vendor relations/ customer-brand interaction or improving access to and control of usage of health-related information.

4.4. Technological readiness

Unsurprisingly, respondents almost unanimously claimed to be technologically ready. More specifically, the survey questionnaire asked responses to four elements:

4.4.1. User identification/ authentication/ authorisation

Responses suggest that this element is well developed and that there are scalable solutions on the market while at the same time, community-driven initiatives are on-going to further refine technologies.

Next to traditional user identification used by the user him/herself for identification on the platform (login name/ ID – or use of national social security or ID numbers, password, accompanied by SMS token or similar), open identification, authentication and authorisation architectures are being used, such as: OAuth, OpenID, OpenID Connect, Kantara UMA[16] (interlinked/ complementary approaches) and Universal Authentication Framework and Universal Second Factor (developed both by the FIDO Alliance), as well as older initiatives such as Mozilla Persona and the Security Assertion Markup Language (SAML, developed by OASIS) and including commercial solutions such as Gigya.

Mydex sticks out by specifying that in light of the multiple protocols currently in use, the multi-protocol support it offers is of crucial importance.

4.4.2. Vulnerability/ security of the architectures

While there are some models considering the decentralised storage of the personal information on hardware controlled by the user ("Freedom Box" by Danubetech, digi.me, commercial reflections by CozyCloud and Meeco to team up with internet service providers in view of equipping the internet access routers with storage capacity for personal information), most models suggest a centralised storage of the information at the platform providers end (cloud-based). This may also be the commercially more promising part facilitating the development of analytics-as-a-service offers potentially necessary to fund in part the platform's operations. Qiy Foundation follows a different model with distributed storage of the data at the original source of collection also in view of offering the exchange of certified documents (in particular originating from public administrations) as a service in the trust framework.

CozyCloud feels that technology is mature at proof-of-concept level, but more work is needed for full-scale role-out, whereas openPDS and Synergetics consider this to be a rather standard challenge.

All replies point to the use of encryption being used for data exchanges inside the platform also as a means to protect the data from outside attacks (next to guaranteeing data use in compliance with the consent of the individual.

[16] Working group chaired by Eve Maler, VP Innovation & Emerging Technology at ForgeRock.

Many providers[17] have designed the platform to be "zero-knowledge" meaning that there the platform provider has no means to access the personal data stored in the individual's 'vault' without the consent of the individual.[18]

4.4.3. Machine-readable expression of privacy preferences and related exchange protocols

This aspect has been subject of a number of scientific projects in the past. Overall, we understand that there are some workable proofs-of-concept, but no approach had yet to sustain the test of being scaled in a real-life environment.

Work is going on in particular in the framework of the Kantara Inititative[19] on identifying and document use case scenarios and specifying policy and technology enablers that allow the exchange of expressed privacy preferences. Work was also on-going in the context of the Liberty Alliance in the past, work now subsumed under the Kantara Initiative, including a specific architecture for "usage directives".
Meeco reports to include a Permission Consent Management layer that generates "contracts" by fields, giving the user to determine duration and terms of the data exchange, including the option to revoke, delete, update and republish the data.
MyWave uses JSON documents containing the metadata indicating the privacy preferences exchanged via the secured and encrypted https protocol.
OpenConsent (formerly OpenNotice) specialises in this area, providing "consent-as-a-service", focussing also on logging and tracking consent, including by developing standards for "consent receipts". Additionally, they contribute to the mentioned sub-group of the Kantara Initiative and aim to support "an international architecture to support ubiquitous machine and human-readable expression of privacy preferences, related exchange protocols in a manner that meets legal notice and consent requirements", aiming for "beta services".

Legal "hackathons" like the one undertaken in the context of the French Open Law project reveal that privacy terms and conditions used on commonly used website are sufficiently similar so as to be structured into a set of re-use conditions.

4.4.4. Technical assurances preventing illicit use of personal data retrieved from a 'personal data cloud'

It appears that most efforts currently concentrate on a two-tier approach:

- **Technical assurances** preventing use of personal information beyond the consent of the individual within the platform/ ecosystem, mostly using **encryption** as a tool with access to decryption keys made dependent on the respect of the stated privacy preferences;

[17] Highlighted in particular by Mydex, digi.me and Meeco, but possibly part of the architectural design of other solutions as well.
[18] We understand that Apple follows this same model.
[19] Chaired by Mark Lizar from OpenConsent (formerly OpenNotice).

- **Legal assurances** (rules governing use of the platform/ participation in the ecosystem) are used to ensure respect for onward downstream use of the personal information;

Respondents take the view that it is currently very hard to provide additional technical assurances downstream. We note an emerging academic literature on and experimentation under the concept of "**data provenance**", sometimes also referred to "watermarking privacy preferences into the data". According to this approach, the privacy preferences are not communicated downstream by "wrapping" them around the data like in the case of using cryptography (the encryption mechanism working as a "box" preventing any access to the data unless a decryption key is applied), but attaching information about the provenance of the data to the data itself in a way that cannot be tampered with. This will not provide with a technical prevention of illicit further downstream use, but serves as a support to audit the compliance of any downstream usage with the privacy preferences stated at the original collection.

5. WHAT DO THE ORGANISATION CONSULTED EXPECT FROM THE PUBLIC SECTOR (AT THE LEVEL OF MUNICIPALITIES, REGIONS, MEMBER STATES, THE EU)?

5.1. What role for public sector organisations in general?

The questionnaire had suggested three areas of potential public sector intervention:

(1) Technical (e.g. set-up of a core platform by the public side with commercial actors offering services on top of them)

Less than half of the responses (10/26) favoured some type of public sector involvement in this respect.

Almost all responses either explicitly rejected the idea of the public sector setting up some type of core platform itself. Responses that elaborated on this matter argued that the public sector itself would not have the sufficient level of trust among citizens or would not be customer-oriented ("person-centred") enough to provide the rich service individuals would expect from a personal information management system.

Only one answer included the interesting idea that there could be a basic service offered by government in a universal service type of arrangement.

However, it was highlighted in a number of responses that government involvement is necessary in the **governance of the trust architecture**, i.e. in the authority that overlooks the rules, standards and protocols applied in the ecosystem. This would become increasingly relevant with a wider adoption of personal information management services.

(2) Financial (direct subsidies for operations, tax breaks, research grants to test pilot applications

21 out of the 26 replies supported some kind of financial assistance.

Most specified that while they expect personal information management services to be financially sustainable in the mid- and long-term, some sort of public money would be needed in order to **catalyse roll-out and reach critical mass**. MiData Coop mentions "loans" as an appropriate funding instrument, indicating the expectation that they would be paid back subsequently.

Financial support to **test pilots with real data and real users** or early-stage models would be necessary. This testing could include also cross-border transfer scenarios. Mydex points out that financial support should not be linked to the use of a specific architectural solution. CozyCloud believes that also commercial applications building on data from personal information management services could also benefit from public subsidies.

(3) Facilitating more wide-spread adoption by top-down implementation

20 replies out of 26 favoured some kind of public intervention either in the form of **leadership by example** or by putting in place the necessary regulatory framework or soft approaches to foster the adoption of personal information management systems, e.g. by making public statements that "personal information management systems are the right thing to do".

A number of responses suggested that public sector organisations should implement personal information management solutions when interacting with citizens in an **eGovernment context**, kick-starting a market. This may even lead to cuts in costs while improving quality of services to citizens through personalisation. We note that one of the UK local government bodies, but also the Slovak, Romanian and Estonian governments joined the evidence-collection process as observers as they are considering building in personal information management solutions in their eGovernment strategies. Another area for top-down implementation are **health care systems**, in particular such systems that have a high degree of centralised control by a public authority, making it easier to impose certain technologies or standards. One response suggested that public sector bodies could offer it to their employees. CozyCloud mentioned **university students** as a target audience, suggesting the public universities would set up personal information management platforms for their students so as to get them used to the approach.

Another role the public sector could play is the issuing of "**verified attributes**" to individuals in order to facilitate personal information management services, a proposal included in a significant number of responses.

On the regulatory front, the importance of the **General Data Protection Regulation** and in particular the right to access one's data and the right to data portability were mentioned. The introduction of such new rights should be accompanied by awareness

raising campaigns. Responses included calls for stronger rules on making the right to data portability work, referring to the **US Blue and Green Button initiatives**. Currently, personal information management services are held back still by the practical problems of accessing personal information. The final provisions on data portability in the future General Data Protection Regulation need to be carefully examined as to their usefulness in practice. Additional work may be needed. Data should be available at least in a machine-readable format, but ideally it would be available online to users identified in real time by standard means and through secure APIs. **Incentives** to companies holding the data need to be reflected upon.

The response by Fondation Internet Nouvelle Génération adds a word of caution, saying that tactically, personal information management services should be presented as a business challenge or opportunity so that inside companies the **business innovators** are tasked to explore their potential. If such personal information management solutions were mandated top-down with an anti-business attitude, this would likely mean the involvement of the compliance department or government relations staff trying to water down any type of obligation. This would represent a missed opportunity.

5.2. What specific role for the European Commission?

The questionnaire suggested three strands of EC involvement:

(1) Support the development of personal information management systems through additional research and if so: In what areas is additional research needed?

While some respondents declared that they believe that enough research had been done and that the focus should now on deployment, clearly underlying their readiness to commercially offer some sort of service – even if not developed to the full extent possible – a significant number of respondents saw the **need for further experimentation at pilot level using real-life scenarios** in order to gain more experiences. The ethical and legal frameworks should also be studied in this context. Such experiments could also deepen the understanding on anonymisation and data aggregation needs so as to develop "personal Big Data" applications and services[20] on top of personal information management platforms data and examine real-life re-identification risks in such cases.

We see no contradiction between the two statements. In fact, commercial deployment will be necessary in order to obtain experiences that can only be obtained once a technology or service goes beyond the phase of piloting into "industrial" production. Also, as shown by the examples given above, certain personal information management services are possible today while certain types of services or functionalities are not.

[20] Understood to be applications or services that provide advice to individuals on the basis of (Big) data analytics applied using the individual data in combination with relevant data relating to peer groups.

Specific areas for additional research are at the technical level, related to legislation and on the business model level:

- **User-managed consent**
  Replies suggest that the management of datasets which are personal but the exploitation of which involves multiple parties (the party having originally collected the data, the third party providing an application on top of the data and possibly intermediary parties, producers of hardware or providers of storage etc.) is complex and potentially needs further study.
  A significant number of replies converged on suggesting that the issue of "user-managed consent" needed more research. Work specifically could focus on:
  - making sure that consent is sufficiently granular;
  - making sure that companies receive legal certainty on consent given in the online world(links to on-going work on "consent receipts");
  - assisting the individual to cognify risks when being asked to express consent by context- and situation-aware support on consent choices;
  - providing for the possibility of delegating consent decisions to individuals or machines, in particular in view of situations when the individual may not have full capacity (important in health contexts); this will require further refinement of machine-readability of privacy notices and consent statements, building on an existing body of work, on the basis of real-life experimentation; scaling machine-readable policies to larger user audiences is a challenge;
  - having more clarity on consent requirements in relation to analytics queries.

  Coelition suggests that any such research should be driven by real-world consent situations. Also more work may be necessary for individual users to signal intents for products of services.

- **Impacts, business models**
  A cluster of responses suggested a number of actions in support of the commercial challenge identified earlier:
  - Gathering of evidence on the economic importance and impact of personal information management services so as to create the evidence-base that will facilitate individual applications for public subsidies or capital investment;
  - nature and potential impacts of alternative business models, revenue streams and funding routes;
  - explore what new services will appear as a result of personal information management platforms;
  - identifying whether there are the risks of digital exclusion as a result?

- **Making the right to data portability effective**

  While many actors believe that the new right to data portability foreseen under the future General Data Protection Regulation (GDPR) will stimulate data inflow into personal information management platforms, some actors wonder whether it will be effective enough also in terms of the practical obligations on data holders to provide for an easy way of extracting data, e.g. through an open and well-documented API.

  Also a word of caution should be added: Data-holding organisations may understand the right to only apply to data transfers between services of a similar kind (e.g. email providers). According to this view it should be examined whether on the basis of this right under the future GDPR an individual could also demand to obtain a copy of his/ her data to be ported into a personal information management platform in view of giving access to such data to third parties;

- A more thorough understanding of **user behaviour** and expectations in relation to personal information management services and platforms;

- **Verified attributes**, including social attributes (such as user behaviour and social relations);

- In the context of improving vendor-relationship management in a privacy-preserving way, more research may be needed on **algorithms** matching user preferences and contextual reputation with various aspects of vendor offerings;

- In addition to research on some of the "components" of personal information management services, additionally further examination of the **integration** (interoperability) of the different "components" such as identity management, centralised authentication, storage, local data analysis, user interfaces appears needed.

Ideally, a **dedicated research programme on personal information management** would be created.

(2) Facilitate interoperability by setting up a process ensuring the emergence of interoperable standards (for representation of data, metadata, for exchange protocols) in order to ensure also the right to data portability foreseen under the future General Data Protection Regulation?

Overall, actors recognise the importance of the regulatory regime (General Data Protection Regulation).

While a significant number of respondents submitted suggestions for concrete areas in which standardisation or at least ensuring interoperability would be desirable, another significant number of actors expressed a general word of caution: Standards rarely lead, but should evolve after a period of competition and complexity. Defining standards is time-consuming and complex and many actors cannot wait for the results of such

processes. Already the announcement of any kind of standardisation process could thus bring innovation to a halt as every actor will not propose new products or services awaiting the adoption of the formal standard. Standardisation should be driven bottom-up rather than top down. Any standard should be an open standard so as to driven down costs of implementation. Standards should not represent a barrier to market entry for small and medium-sized enterprises. As a start an overview of existing standards in use today will be required. Healthbank Cooperative considers that too many compromises are necessary in any standardisation effort undertaking in order to achieve interoperability which in general presents the risks of inhibiting innovation as such compromises may reduce the richness of information/functionalities.

On the other hand, the emergence of de facto standards in closed ecosystems may make it necessary so as to prevent lock-in effects. Fing suggest that another criterion is to assess the maturity of the solutions on the markets. Only such issues should be addressed by standardisation activities that have been properly tested enough in real-life situations or contexts. MiData Cooperative believes that the need for standardisation will result from secondary use of the data stored on the personal information management platforms as this will highlight the areas in which data integration is most interesting.

In the meantime multi-protocol support and work on mappings between different standards will be sufficient.

Items for potential standardisation resulting from the responses are:

- Work on a "**common personal data model**", including data formats. In this context, the UK Digital Catapult points to on-going work involving itself, Open Identity Exchange and the Open Data Institute. The EC could aim to consolidate those existing initiatives into a single "framework";
- **Data portability**: Data should be accessible via a well-document API in a machine-readable format and should be provided for free;
- **User-managed access** and legal interoperability: Additional research pending (see above), the on-going work notably in the Kantara UMA initiative could be built upon; a future evolution of the General Data Protection Regulation should also support more granular consent options; mappings between Kantara UMA consent concepts and "legal constructs".

(3) Soft promotion and what exactly could be done?

Respondents suggested a number of action streams which can be clustered as follows:

- There was a strong call – in particular at the round table – on the EC to publicly support personal information management solutions and the nascent industry; such a public endorsement could take place as a follow-up to the GDPR adoption and/or or in the context of the DSM/Free Flow of Data Initiative.
- Promotional activities with respect to prospective individual users of personal information management services (information about online rights, data protection regulation) so as to increase the number of (potential) users.

- Promotional activities with respect to organisations, such as meetings between data-holding companies and providers of personal information management solutions; Cozy suggests that the threat of "uberization" may be instrumental in attracting companies' interest;
- Community-building through regular meetings among providers (or sub-sets) in order to discuss and share experiences, methodologies as the market for personal information management solutions matures;
- General policy messages, white papers etc that can catalyse or accelerate a process towards wider use of personal information management services; the message should be on "data empowerment" not on "data protection".
- Require "data usage reports" to be established in common format, requiring organisations to report on data they hold, on who they share it with and what purpose is made of the data shared so as to improve the functioning of the transparency and access rules of the General Data Protection Regulation.

6. COMMUNITY-BUILDING

The evidence-collection process revealed that there is a community-building effort on-going, accelerated by the convening of meeting of 27 November 2015 to which bi- and multi-lateral meetings among players were organised back-to-back. Fondation Internet Nouvelle Génération and Helsinki Institute of Information Technology are closely cooperating in further studying the field, the framework conditions and offering additional work streams with commercial providers. The UK Digital Catapult is also interested in being involved.

As a result, three follow-up workshops are scheduled for 2016 hosted by Fondation Internet Nouvelle Génération (April 2016), Helsinki Institute of Information Technology (back-to-back with their international MyData2016 conference end August/ beginning of September) and the UK Digital Catapult (autumn 2016).

CONNECT/G3 is keeping informal links with all actors concerned so as to ensure that all actions are complementary and not overlapping.

7. CONCLUSION

The sector is still in its early stages. There are a number of players that either already have or are about to launch commercial offerings. Still, many of the actors are relatively small in size, meaning that there is a clear challenge to roll-out personal information management services to a mass market. Players signal that access to capital is difficult, also because there is limited evidence available on the economic importance of enabling "personal Big Data" applications. On the other hand, we noted that in particular telco providers are experimenting with a personal information management service offer.

Actors expect that the enhanced right to data portability and the fact that rules on consent as a legal grounds for data processing remain largely the same as under the 1995 Directive will give an additional push to a more wide-spread adoption of personal

information management services. The applicability of the right to data portability, however, needs further study.

There is an emerging community that organises itself in view of exchanging business strategies but also collaborate on interoperable standards.

More work is needed on a number of fronts and the following lines for potential action were identified:

- Political support and public endorsement of the concept of personal information management platforms; such work should include providing additional economic evidence on the importance of the market for applications that make use of the opportunity of integration of personal data coming from diverse sources;
- Further examination of the role of public sector organisations as part of the governance of personal information ecosystems so as to ensure trust;
- Practical support for community-driven collaboration (coordination, making available meeting rooms);
- Further evidence on the right to data portability in particular assessing its applicability in the context of enriching data content of personal information management platforms and identifying potential technical or other practical barriers in view of identifying potential additional measures to make the right effective in practice;
- Support for additional experimentation and piloting of personal information management platforms;
- A number of specific research challenges, notably in respect to the concept of consent and its implementation in practice;
- Kick-starting the roll-out by supporting governments and administrations to use personal information management platforms when managing citizen's data in the context of eGovernment.