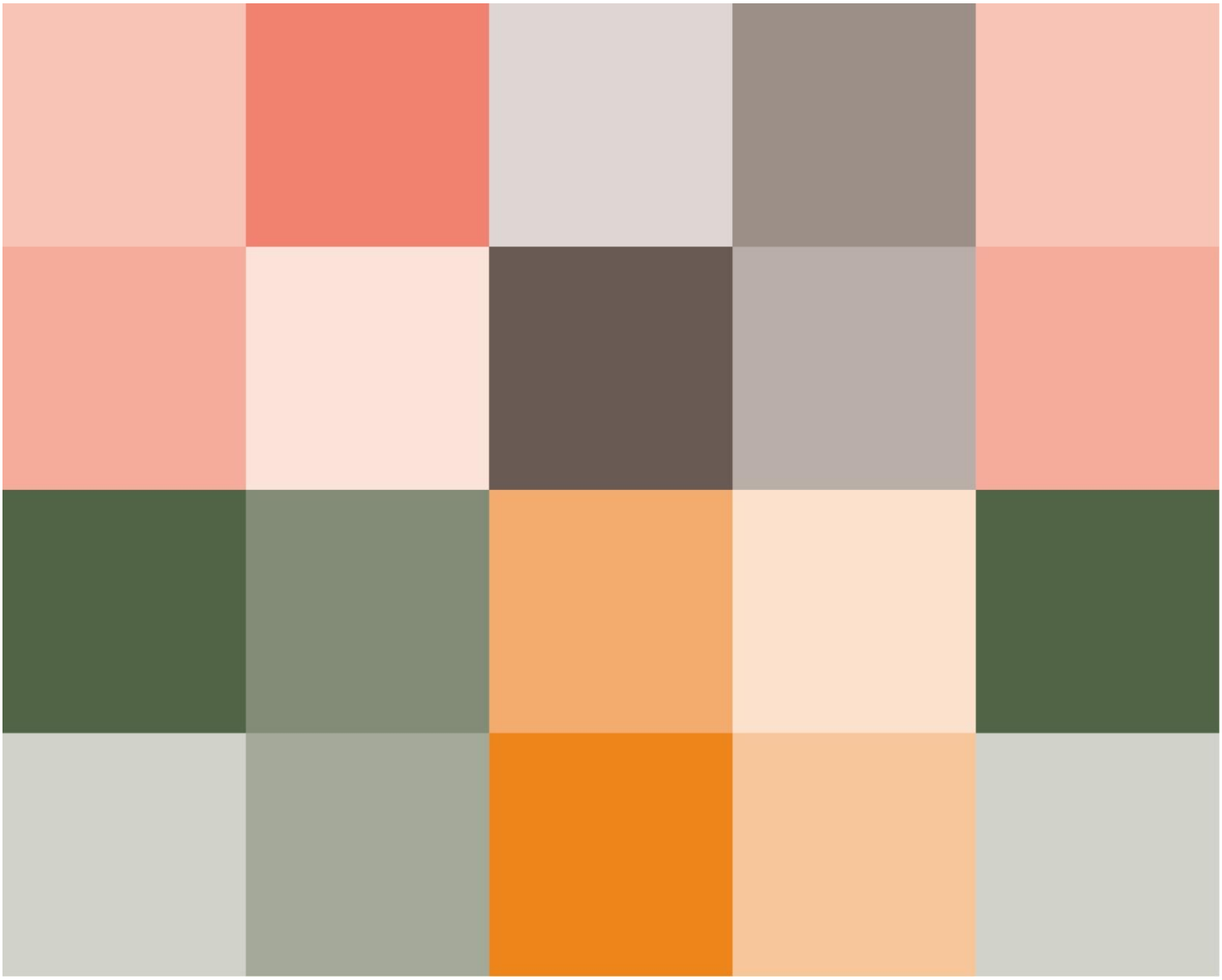


Commission to enable solutions for individuals to be able to have insight and control over data kept about them

I2020/02024/DF

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Preface

In July 2020, the Swedish Public Employment Service, the Swedish eHealth Agency, the Agency for Digital Government (DIGG) and the Swedish Tax Agency were collectively tasked with showing how an individual's ability to have insight and control over data that have been stored about them by the public sector – and, in the long term, also data about the individual that are stored in the private sector – can be enhanced.

DIGG was responsible for overall coordination of the assignment. The Swedish Public Employment Service was responsible for developing the proof of concept. Work on this report has been done collaboratively, so the first-person plural ("we") has been used throughout.

A multi-agency steering committee has been connected to the assignment. The steering committee consisted of the following people: From the Swedish eHealth Agency, Director for Legal Affairs Erik Janzon participated until 2021-03-01, when Director for Legal Affairs Maria Jacobsson took over. From DIGG, Delivery Manager Viktoria Hagelstedt participated until 2021-02-01, when Operational Area Manager Mats Snäll took over. From the Swedish Tax Agency, Andreas Elvén participated, and Gregory Golding participated from the Swedish Public Employment Service.

Decisions regarding this report were made by the Director-Generals of each respective authority. For the Swedish eHealth Agency, Janna Valik; for the Swedish Tax Agency, Katrin Westling Palm; for DIGG, Anna Eriksson; and for the Swedish Public Employment Service, Maria Mindhammar.

Theodor Andersson (DIGG), Jan Sjösten (the Swedish Tax Agency), Hans Ahlqvist (the Swedish Public Employment Service) and Bessam Saleh (the Swedish eHealth Agency) were rapporteurs.

Stockholm, 1 June 2021

Summary

The Swedish Public Employment Service, the Swedish eHealth Agency, the Agency for Digital Government (DIGG) and the Swedish Tax Agency have been tasked by the government to investigate how the situation regarding an individual's ability to have insight and control over data that have been stored about them by the public sector – and, in the long term, also data about the individual that are stored in the private sector – can be enhanced.

Who has control over an individual's data is a question that will become increasingly important as time goes by. Digitisation of the Swedish public sector has long been based on the needs of each authority, and significant areas of digital development have been motivated by increased efficiency and productivity. Subsequently, the public sector was increasingly characterised by efforts that prioritised the needs of individuals for simple, quick and accessible services. It is an important development, but is lacking because these efforts were largely based on the authorities' own operations and their respective areas of responsibility. The latest development is for services to be based on so-called life events that individuals go through at various stages of their lives. In that way, the public sector can provide private individuals with more unified, user-centric and integrated services that stretch across the boundaries of the authorities and sectors. This development, which is driven by various initiatives in the form of policy documents and strategies at the national level as well as from the EU, bring to the fore new needs and possibilities, as well as challenges.

In order to succeed in delivering community services that correspond to the expectations of private individuals today and in the future, it is becoming increasingly evident that data must be seen as a strategic resource. Data records in use in the Nordic countries – not least of which Sweden – are unique not only because they have existed for such a long time, but also because authorities find support in national legislation for collecting and maintaining a large quantity of data. This has resulted in there being a good basis for a data-driven administration that can use relevant data when needed, provided that privacy and security requirements are met.

Allowing individuals to have greater insight and control over data that have been collected about them in both the public and private sectors can generate considerable economic and other value.

With the help of data controlled by the individual, companies and organisations could create innovative services for private individuals and other companies, thereby contributing to developing the Swedish "data economy".

In order for authorities to be able to continue to provide new services that live up to the increased expectations of private individuals, new conditions need to be created.

The transmission of data, which is at the very core of modern services, needs an infrastructure that can connect different sectors together. It is important that efforts relating to the common digital infrastructure amongst public authorities can be developed in order to also meet the needs of individuals for having insight and control. If, in the future, data management increasingly makes use of consent as a legal basis for processing personal data, then the digital proficiency of private individuals will also be an important prerequisite. In order to maintain trust in the public sector, and in the long term, also private companies that process large quantities of personal data, issues of insight and control – that is, how and by whom the data are used – become increasingly important.

The external analysis has strengthened the view that an individual's increased insight and control over personal data is a matter of priority not only for Sweden but also for many other countries. The EU and increasing numbers of Member States are therefore trying to find new opportunities to give private individuals control over their personal data. In order to succeed in this, technical solutions need to be combined with legal frameworks and secrecy and privacy safeguards that support such a development. It is also important that private individuals understand the meaning of data protection and have sufficient digital literacy to act on the opportunities available to them for protecting their personal data stored by various parties. Our external analysis shows that no individual country, whether within or outside of the EU, has completely succeeded in this.

We have developed a Proof of Concept (PoC) that shows how an individual can retrieve data from a few authorities to create a CV with the Swedish Public Employment Service containing validated information from different sources, which can be used to help the person in looking for employment. This makes the information more credible and also makes it possible for individuals to be able to streamline their application process. We see that the proposed solution in the proof of concept allows individuals to be able to have insight and control over data about themselves in the public sector, and in the future, also the private sector, and we also see how this can provide clear added value for the individual; in this case facilitating a job search.

In order to try to highlight the Swedish position with regards the individual's increased ability to have insight and control over their personal data, we present a model that shows how a common data ecosystem amongst public authorities could be designed. It shows how future data flows, under the control and oversight of the individual, could contribute to increased efficiency, individual centricity and innovation. The model is conceptual, which means that several prerequisites need to be added or changed. In order to make the future possibilities tangible, we have produced a visualisation of a hypothetical future service that would meet the needs of individuals in the life event of being on sick leave.

In working with this government assignment, we have noted several legal challenges that need to be investigated further before ideas about an ecosystem, insight and control can become a reality. There is a potential conflict between an individual's entitlement to insight and control on the one hand, and the prerequisites for authorities to realise such insight and control on the other.

It is not entirely clear how Sweden's residents want insight into and control over data to materialise. We therefore suggest that a survey of the population be conducted to further investigate how tools for insight and control can be designed that are also digitally inclusive.

We believe that the conceptual model presented in this report could rely on the common digital infrastructure amongst public authorities that is now emerging.[1] We assess that the building blocks of My Representatives, My Cases and My Profile can provide for the data overview that we believe is needed. The Indexing building block is also an important prerequisite in the continued work. The question of an individual's insight and control can therefore benefit from further development within the common digital infrastructure amongst public authorities.

The coso-called eget utrymme [user area] at a public authority is currently used by agencies to provide services for private individuals and businesses. Several legal issues are currently unresolved regarding the prerequisites for making use of a user area for increased insight and control. We therefore recommend that these be further investigated. An important part of this work is to examine the legal situation and the limitations regarding the scope of controllership in relation to the user area. Another important part is to investigate how the user area can be designed in such a way as to support user-centric data sharing within sectors or during life events. This work can suitably be done in consultation with the Swedish Authority for Privacy Protection in order to bring about a proactive approach, and so as to more quickly highlight needs for adjusting regulations.

Today, the way that authorities process personal data is regulated by means of sector-specific legislation. The legal status for the digital transmission of information and the possibilities of providing individuals with insight and control can be considered uncertain. We therefore suggest that an impact analysis should be conducted with regards to expanding the service obligations, together with a review of the special data protection regulations (data registry laws) and the possibility of disclosing data in electronic form.

[1] The Swedish Government (2019) *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte [Assignment to establish a common digital infrastructure for information exchange amongst public authorities]* Reg. No.: I2019/03306/DF

Innehållsförteckning

1 Introduction

1.1 Background

Large quantities of data about individuals are processed by public administration, for which there is support in statutes or agreements. The public sector often not only has the right but also an obligation to process personal data.

The EU General Data Protection Regulation (GDPR) applies to all organisations and industries that process personal and sensitive information about individuals. Amongst other things, it gives individuals the entitlement to receive extracts from registers, i.e., information about what personal data is processed and in what way, as well as the right to request that personal data be deleted or transferred from one party to another (data portability). However, to the individual, it can be perceived as difficult to gain an overview and have insight into the information that various parties have about them. In many cases, individuals have limited possibilities to in a simple manner show digitally, that data are incorrect or request that data from various interested parties be deleted.

It would make things easier for individuals and introduce efficiency improvements for the public sector if it were possible for another party to reuse information already possessed by an authority as the basis for making decisions or taking certain measures. But it is unclear exactly how this will be done and what prerequisites need to be in place for such user centricity. As part of this assignment, we have explored obstacles and opportunities for improving an individual's insight into and control over data that the public sector holds on the individual.

1.2 Assignment

The government has tasked the Swedish Public Employment Service, the Swedish eHealth Agency, the Agency for Digital Government (DIGG) and the Swedish Tax Agency with conducting an external analysis and developing a proof of concept (PoC) that shows how it is possible to increase opportunities for individuals to

have insight and control over the data held on them in the public sector and, in the long term, also within the private sector.[2]

1.3 Outline of the report

The report consists of seven chapters. The introduction contains recommendations for continued investigation and a description of how the assessment has been carried out. Chapter 2 consists of a needs analysis that has been conducted, which, amongst other things, sheds light on civic attitudes towards data sharing and an increased personal responsibility for it. Chapter 3 describes developments in the external environment. This includes work that is under way at the EU, UN and OECD levels, as well as insights from initiatives and projects that were conducted or are currently ongoing in other countries. Chapter 4 contains a brief account of the common digital infrastructure amongst public authorities that is currently emerging in Sweden for the exchange of information. A description is also given of the thinking behind digital ecosystems, and examples are given for how certain services today provide insight and control. Chapter 5 presents the proof of concept that the Swedish Public Employment Service was tasked with developing as part of this commission. Chapter 6 describes a common model amongst public authorities for how an individual can be given insight and control over data about themselves, and how the model can be applied during a life event in order to facilitate the individual's interactions with interested parties in the public and private sectors. Finally, in chapter 7, we highlight the needs that must be addressed and make a number of recommendations for further work.

There are four annexes to this report. The purpose of dividing the report up in this way is to create a condensed main report that highlights key points from the external analysis and exchanges of experience domestically. Annex 1 contains the basis of the needs analysis, which consists of a review of a number of Swedish and foreign citizen surveys. Annex 2 consists of external environment monitoring of the EU, UN, OECD, and seven countries that were analysed within the scope of the assignment. Annex 3 is a document containing an extensive legal analysis, and Annex 4 is a more detailed technical description of the proof of concept that was developed under the leadership of the Swedish Public Employment Service.

[2] https://www.regeringen.se/4a647d/contentassets/84872b67c0c8480a9544dc076fa20aef/uppdrag-att-mojliggora-losningar-for-individen-till-kontroll-och-insyn-av-data-om-individen.pdf

1.4 Implementation of the assignment

DIGG was responsible for overall coordination of the assignment, and the Swedish Public Employment Service was responsible for development of the proof of concept. The assignment has otherwise been carried out as a collaborative effort by the authorities.

Initial external environment monitoring focused on reviewing various reports, strategies and other publications from the EU, UN and OECD in order to determine if there is consensus regarding the issue of whether individuals are entitled to increased insight into and control over the data stored about them, and how well the technological development and discussions on policy, management and control agree with the vision for how this insight and control will be given to and managed by the individual.

Examples from a number of different countries (Finland, France, Norway, Denmark, the United States, the United Kingdom and India) were also analysed to emphasise various aspects of insight and control, such as technical solutions, legal aspects, the involvement of trade and industry, and the value of political governance.

One representative from each authority formed a steering committee and were able to follow ongoing developments of the work by means of regular meetings and status checks. The steering committee were mandated to make decisions on matters raised by the working group and to make recommendations themselves regarding the composition and direction of the work.

In order to organise work on the assignment, a number of special working groups were also created that had specific focus areas and regularly coordinated their efforts with the primary working group for the assignment.

1.4.1 Legal work

The legal aspects constituted a special focus area for this assignment, and a special working group was formed consisting of lawyers from the authorities collaborating within the assignment. The legal discussions that the group have been engaged in have been based on the efforts made as part of the assignment to develop a generic model and the life events that have been used for developing the proof of concept and the sharing of information that these involve.

The efforts of the working group are presented in their entirety in Annex 3, *Comprehensive legal analysis of the possibility of increasing insight and control for individuals.* The conclusions that the working group have come to in their analysis of the legal regulations and the limitations and possibilities that these bring about with regards to sharing information according to the conceptual model have been taken into consideration when creating the proof of concept.

In addition to the comprehensive analysis presented in Annex 3, there is also a special legal analysis of the technical proof of concept (life event: *starting work*) that the Swedish Public Employment Service has been responsible for. The legal analysis presented in connection with the proof of concept is anchored in the general legal analysis made in Annex 3.

1.4.2 Work relating to life events

In order to understand the needs of individuals and find development areas that can simplify day-to-day life for many, it is important to start from the perspective of life events. For this reason, the *Life Events* working group was created, which made use of the work of eSams[3] regarding how authorities can base their work on the personal circumstances of citizens.[4] Examples of categories of personal circumstances include health, work and education. Incidents occur in an individual's life that affect their personal circumstances, and these are called life events. Examples of life events include *being on sick leave*, which is linked to the personal circumstance, *health; starting work*, which is in turn linked to the personal circumstance, *work*, and so on.

The working group focused on two life events – *starting work* and *being on sick leave* –, which allow for a necessary limit to be set regarding the quantity and type of data included in the analysis. Activities involving the sharing of data and the number of parties involved have been limited in order to simplify the analysis.

When a life event occurs, the individual does something, which is termed an action in the report. Examples of actions in the *being on sick leave* life event could include *contacting healthcare services*; and for *searching for work*, the action is linked

[3] eSam is a member-run programme for collaboration between 29 authorities and SALAR; its central objective is to help meet the needs of private individuals and companies to be able to carry out various errands at authorities and municipalities.

[4] eSam (2016) *Behovsdriven utveckling – en vägledning. [Needs-driven development – guide].*

to the starting work life event. It was the needs that guided the life events analysis rather than the assignments of authorities or organisational structures. The goal was to make things simpler for the individual.

The *starting work* and *being on sick leave* life events were chosen according to the following dimensions:

- cross-agency and cross-sector
- create considerable added value for the individual
- insight and control should be able to be applied to other personal circumstances and life events.

Work regarding the *being on sick leave* life event resulted in a visualisation that illustrated a future scenario and contains no technical functionality. The conceptual model for a user-centric data ecosystem that was developed as part of this commission from the government forms the basis of the future scenario that is described as a *new situation*.

Work on the *starting work* life event forms the basis for the proof of concept described in the sections that follow.

1.4.3 Work relating to the Proof of Concept (PoC)

A working group has developed a proof of concept (PoC) that shows how increased possibilities for insight and control over data about the individual kept in the public – and in the long-term, also the private – sector can provide clear added value for the individual. Privacy and data portability are the core of the assignment, and therefore also the legal situation for processing and sharing personal data.

The Swedish Public Employment Service was responsible for implementing and supplying the technical proof of concept for the *starting work* life event.

1.5 Boundaries

Life events The choice of life events has focused on those related to health and the labour-market. These are two areas of high priority especially with regards to the sharing of data because there are considerable socioeconomic gains to be made.

Additionally, in times of pandemic, these two areas are highly relevant, since both the health sector and the labour market have been particularly hard pressed by the consequences of the pandemic with regards to the possibilities of good health and

secure conditions of employment.
The life events have been abbreviated to specific phases within larger life events.

Contacts with trade and industry For the authorities, the assignment includes reasoning on the possibilities of allowing individuals to be able use digital tools to have increased insight and control over data about themselves stored in the private sector, and therefore involves a dialogue with relevant entities in the sector. However, the primary focus has been public administration, and the majority of consultations with external parties has been managed as part of efforts to develop the proof of concept for the *starting work* life event.

The boundaries set in the number of contacts with entities in the private sector and the number of areas that have been investigated are due to the complexity of the assignment. An active choice has therefore been made to prioritise the role of public administration in a user-centric digital ecosystem. There is a need for continued work with more open and broader contacts with trade and industry, but only after the legal restrictions and possibilities have been clarified. The external analysis has shown that collaboration from trade and industry is most useful when public entities better understand the possible implications of the solutions proposed for businesses and their processing of customer data. It is also desirable to have a clear legal situation and environments for experimental innovation efforts, such as regulatory sandboxes or greenhouses.

1.6 Key concepts

There are three principal concepts in the report, and these are insight, control, and personal data or personal information. The term user-centric also appears in several places and is accordingly defined below. Other key concepts that are used in order to describe various parts of the conceptual model for an individual's insight and control as described in Chapter 6 are described in connection with that section, especially sections 6.1.1 – 6.1.3.

Insight In this assignment, insight means that individuals are able to visualise or otherwise understand the type of data kept about them by whatever organisation is holding the information in an easily understandable and unified manner, as well as being able to see for what purposes the information is collected, and on what legal basis it is processed there.

Control Control refers mainly to possibilities for an individual to be able to digitally access their data and request corrections, deletion or transferral of data to and from the entity that has it.

Personal data and personal information Personal data means all information relating to a living, identified or identifiable individual. Various types of information that can, together, result in a certain person being identified, are also personal data. This may include identifiers, such as a name, an identity number, location information, or online identifiers or one or more factors that are specific to the natural person's physical, physiological, genetic, mental, financial, cultural or social identity.

User-centric User-centric means that services are based on the needs of individuals and allow them to participate more in the processes.

2 Observations from the needs analysis

It was considered important to include in this assignment the purpose of conducting an analysis of the opinions of private individuals regarding how data about them are processed and shared by the public and private sectors. A citizens' perspective is often lacking, even though it is the individual citizens who are expected to take greater personal responsibility for data about themselves and for data generated by their digital interactions with public and private entities. For a more detailed review, see Annex 1, Needs analysis and citizen's perspective.

2.1 Summary of observations from the needs analysis

- The privacy paradox means that increased insight does not necessarily result in a change in behaviour in those who state that they are concerned that they lack insight or control over the way their personal data is used.
- Most citizen surveys show that the public sector has an important role to play with regards to legitimising new methods of sharing and using data. Trust in the public sector is an important aspect of how private individuals view being part of a data-sharing ecosystem that also includes private companies.
- Increased control over an individual's own personal data is generally desirable, but few are aware of how this control can be exercised or whether they wish to take upon themselves greater responsibility for sharing data that is necessary for efficient public services.
- Calculations from the UK show that there is considerable economic value in shifting towards increased data portability. There is a need for this part of the needs analysis to be investigated further according to the circumstances and possibilities in Sweden. The willingness of individuals and organisations to pay for the services that a provider of "Personal Information Management Systems" (PIMS) can offer needs to be quantified.

2.2 Trust, attitudes and data protection in brief

Two events in recent years can be considered to be of particular significance to the discussion regarding processing personal information on the internet. The first of these is the General Data Protection Regulation (GDPR), which came into force in 2018. The second is the incident regarding the Cambridge Analytica firm that collected personal information about millions of Facebook users for the purpose of influencing the outcome of the United States presidential election in 2016. These events have resulted in the question being raised as to what an individual is willing to approve in terms how personal data are collected, used, and resold by private companies in return for access to their digital services.

The way that organisations use personal data affects the level of trust people have in them. Shortly after the Cambridge Analytica incident, Novus conducted a survey in which a third of Swedes stated that they would change their behaviour, such as by no longer taking personality tests or quizzes on Facebook. A similar proportion considered leaving Facebook altogether, but very few carried through on the matter.[5] In general, people are concerned about their privacy, but they rarely take the necessary measures to protect their personal data. This disparity between attitude and actual behaviour is called the privacy paradox. According to this paradox, insight into the way personal data are used does not necessarily result in a change in behaviour, even if people are worried that they lack control over personal information and how it is used.

According to the *Delade meningar [Diverging views]*[6] survey, for example, just four percent of participants asked for access to their personal information.

There are clear geographical variances across different parts of the world with regards to confidence that personal data will not be misused. According to *The Global State of Online Digital Trust* report, people in Europe have a considerably lower degree of trust that their personal data will not be misused by businesses than the rest of the world.[7] This level of trust has also diminished over time. One possible explanation highlighted in the report is that European laws aiming to protect the basic rights of individuals are perceived to be under threat from the

[5] SVT (2018) *Svenskarnas förtroende för Facebook rasar [Swedish trust in Facebook is plummeting]*, published 2018-03-29

[6] Delade meningar, svenska folkets attityder till digital integritet 2020 [Diverging views – Swedish attitudes to digital integrity, 2020] deladeMeningar2020_Web_1-9A.pdf (insightintelligence.se)

[7] https://docs.broadcom.com/doc/the-global-state-of-online-digital-trust

companies that increasingly make use of personal data for various purposes. Whilst people have a relatively low level of trust in the way that businesses process personal data, more and more companies are of the opinion that their trust capital has increased. Consumer trust in the way that businesses process personal information must improve if businesses wish to grow.

The way private companies process personal data is what mainly concerns people in Sweden, and the general concern that data will be used for purposes for which the person has not approved or has no insight into doubled between 2015 and 2020. Today, 49 percent of the population share that concern.[8] The feeling of security does not necessarily increase if personal data are anonymised because businesses are then not obligated to provide information on how the data is used. Although most surveyed have a relatively high level of trust in the way that government entities process personal data, a clear majority feel that sharing data is something done out of compulsion rather than voluntarily.

The OECD identifies trust in the government as an important factor that is decisive with regards to what the attitude of citizens will be towards the handling of data. Responsiveness, decisiveness and reliability with regards to providing public services and foreseeing future needs are crucial for increasing trust in the institutions.[9] In this respect, Sweden is a so-called high-trust society. Confidence and trust in the public sector have traditionally been linked to how well schools and healthcare services are perceived to be operating. In a time of digital transformation, the ability to deliver well-functioning, safe, reliable and transparent digital services is also a significant contributing factor to trust in a public entity. In order to retain trust on the part of private individuals, the way the public sector manages citizens' data is key. This is confirmed by the Swedish Authority for Privacy Protection in its 2020 privacy report,[10] in which it is also determined that this commission from the government to enable solutions for individuals to have insight and control over personal data will likely need to be followed up with additional assignments or investigations to strengthen the ability of individuals to exercise control over their own data.

---

[8] Delade meningar, svenska folkets attityder till digital integritet 2020 deladeMeningar2020_Web_1-9A.pdf (insightintelligence.se)

[9] https://media.sitra.fi/2020/10/08100935/towards-trustworthy-health-data-ecosystems.pdf p.18

[10] https://www.imy.se/globalassets/dokument/rapporter/integritetsskyddsrapport2020.pdf

2.3 Patterns in citizen surveys

It is not readily apparent that control over personal data increases an individual's empowerment in relation to public and private entities. If individuals take on additional responsibility for managing their data, they may give in to a feeling of hopelessness. This "digital resignation" arises when a person does not believe that public or private entities will make changes in the way they process data regardless of the actions taken by the individual. The individual's ability to act is also perceived as considerably limited, since the majority feel that they share information mainly because they are forced to do so.[11]

One conclusion that can be drawn from this is that, whilst general digital maturity – required in order for citizens to be able to make informed decisions about data sharing – is strengthened, the trust capital on the part of citizens should also be built up by public administration by means of transparency that gives the impression of reliability and helps individuals understand why data is being shared.

In one comprehensive British study,[12] a clear majority preferred the option of sharing personal data that involved government regulation and oversight of the data-driven systems (public and private) that process data on individuals. Choices for control were based on a default option for sharing in which all data collection is stopped until individuals have time or the desire to choose how and when their data should be shared; a so-called opt-out alternative.

2.4 Technical solutions for trust, insight and control

In recent times, new technical solutions have been presented that attempt to manage the issue of trust by giving individuals increased control over their data along with increased insight into how data are shared, to whom, and for what purpose. Personal Data Stores (PDS) are one such solution, and the Solid platform, created by founder of the World Wide Web Sir Tim Berners-Lee, is considered in section 4.3.6.

---

[11] Delade meningar, Svenska folkets attityder till digital integritet 2020 deladeMeningar2020_Web_1-9A.pdf (insightintelligence.se) p. 16

[12] Public perceptions of good data management: Findings from a UK-based survey, Hartman, Kennedy, Steedman, & Jones, 2020; Steedman et al., 2020, pp. 8-21

A PDS is intended to provide an individual with a greater ability to protect their data and privacy whilst simultaneously improving the possibilities for trade and revenue generation from personal data. Previously identified problems remain, however; namely, the fact that managing one's own data will require a great deal of time, and that encountering difficulties using various features can cause irritation and stress. There is a pronounced concern about being overburdened by requests for access to data, and here, too, there is a desire to be able to disassociate oneself from the responsibility by outsourcing it to a trusted intermediary, even though such an entity does not currently exist. Neither has the solution succeeded in creating an increased feeling of security amongst surveyed individuals who feel that they lack legal protection if a dispute were to arise or if a non-authorised use of personal data is discovered. In summary, the surveyed individuals advocate a method that gives people control over their data, but the solution should include an accompanying regulatory division, perhaps governmental, that can provide support to individuals in actually supervising the management of data and in cases involving legal disputes with entities included in the data-sharing ecosystem.

2.5 The economic value of personal data mobility

In its data strategy, the European Commission has stated that great value can be achieved by allowing individuals to have increased control over their data. Consideration for consumer influence is part of the reason for the provisions on access to and reuse of data in the Payment Services Directive. Similar to what is advocated by the MyData movement and others, the view of the Commission is that tools and methods allowing people to make detailed decisions about what is done with their data will provide significant advantages to individuals, including financial benefits.[13]

In a 2018 report from the UK Department for Digital, Culture, Media & Sport (DCMS), an examination was made of the potential for stimulating innovation and competition through personal data portability; that is, transferring personal information from one party to another.[14] If personal data from the public and private sectors could flow through a secure system that gives individuals control of their data, the economic impact (in the form of increased productivity and

[13] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52020DC0066&from=EN p. 12.

[14] Department of Digital, Culture, Media & Sport (2018) *Data Mobility: The personal data portability growth opportunity for the UK economy*

competitive advantages) would amount to approximately £27.8 billion, which would correspond to 1.5 percent of the GDP. There are great uncertainties connected to this estimate, and it is based on an early stage; that is, before innovation based on this personal data mobility has had time to create new uses.

An earlier study focused on estimating the potential market value in the United Kingdom for so-called Personal Information Management Systems (PIMS).[15]According to their investigation, organisations were willing to pay between 35 and 60 SEK per relationship, to gain authorised access to an individual's data and have authorised communication with customers. It was also estimated that each individual in the UK maintains between 30 and 100 relationships with banks, applications, retailers, authorities and other organisations. By combining these two estimates with the number of adults and households in the UK, the value of the PIMS market was estimated to amount to approximately 135 billion SEK in the UK.

[15] Ctrl-Shift, *Personal Information Management Systems: An analysis of an emerging market*, 2014.

3 Observations from the external analysis

The most important insights and experiences from the reviewed supra national and intergovernmental organisations are summarised for each organisation. This is followed by a presentation of different countries, of which Finland is reported separately. For more detailed information and analysis, we refer to *Annex 2 – External Analysis*, where the review of each country is presented separately.

3.1 The position of the EU with regards to insight and control

- The EU Data Strategy established that it is in harmony with the General Data Protection Regulation to allow users to be able to influence their own data and to give them the possibility of asserting their rights with regards to the use of the data they generate.
- This possibility is attributed to tools and methods that allow for detailed decisions to be made regarding what is done with the information. These tools are described without details such as personal data spaces.
- The legal basis for sharing data between private and public entities and for an individual's ability to have increased control over this data flow is not specified, although several future investigations will clarify rules, responsibilities and possibilities.
- The EU's ultimate objective is to take advantage of the benefits of improved data use, where data that includes personal information is secure, but can nevertheless be used for promoting growth and generating value in an ecologically sustainable manner.
- Standardising interfaces for accessing data in real time and making it obligatory to use machine-readable formats for data from certain products and services are considered to be essential prerequisites.
- The EU General Data Protection Regulation grants extended rights to individuals, who must be able to exercise their insight and control over their personal information. This also involves increased obligations for everyone processing personal information.

- Systems for personal data mobility are enablers for insight and control, and these can be created according to:
  - Requirements and standards for compatibility in accordance with the FAIR Guiding Principles of findability, accessibility, interoperability and reuse.
  - The Single Digital Gateway regulation and the EU building blocks that seek to ensure that citizens, businesses and administrations benefit from seamless digital public services from anywhere in Europe.

3.1.1 The EU Data Strategy

The EU strategy for data[16] involves political measures and investments in the data economy over the next five years. The reason for this is that there is understood to be a potential for economic growth when more data are shared between different sectors, between public entities and across national borders within the EU. Strict data protection regulations are ethically justified but can also be used as a tool for ensuring trust on the part of the general public towards sharing personal data within the EU. It can also be viewed as a separator and potential competitive advantage over the United States and China, both of which are considered to lack sufficient guarantees regarding privacy for individuals.

A framework and infrastructure are needed for ensuring access to data that supports the creation of European data pools, which allows for big data analysis and machine learning. The Data Strategy further recommends the implementation of sectoral reviews, where legal and other obstacles for using data and data-based offerings are identified. A forthcoming review of the General Data Protection Regulation is also expected to result in further measures for strengthening trust in the use of data in Europe. Additionally, in 2022, the European Commission will issue a rulebook for cloud services that will be a compendium of existing codes of conduct and certifications regarding security, energy efficiency, service quality, data protection and data portability.

[16] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, Brussels, 19.2.2020 COM (2020) p.10

According to the EU Data Strategy, it is in harmony with the General Data Protection Regulation to allow users to be able to influence their own data and to give them the possibility of asserting their rights with regards to the use of the data they generate. The strategy highlights the fact that there are tools and methods that allow for detailed decisions to be made regarding what is done with the information. These tools are described without details such as *personal data spaces*.

According to the Data Strategy, these tools have enormous potential but must be able to handle consent, applications for managing personal information (including completely decentralised solutions built on blockchain technology), and cooperatives or trusts for personal data that serve as neutral intermediaries in the personal data economy. [17]Standardising interfaces for accessing data in real time and making it obligatory to use machine-readable formats for data from certain products and services are considered to be essential prerequisites.

Investments for expanding the next generation infrastructure for handling data will be coordinated with relevant authorities in the Member States and by means of investments through the structural and investments funds. During the 2021–2027 period, funding is provided for infrastructure, data sharing tools, architecture and control mechanisms for robust data-sharing ecosystems and artificial intelligence.

Based on ongoing work on the European Open Science Cloud, the Commission will support the establishment of nine common European data spaces. These include common European data spaces for public administration. Measures taken for the public administration data space focus on legal data and that from public procurement. Other areas of general interest are also included, such as the use of data for improving law enforcement within the EU, which must be done in accordance with EU law, the principle of proportionality and the data protection rules. The area is considered to be an enabler for innovative so-called GovTech, RegTech and LegalTech applications.

[17] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, Brussels, 19.2.2020 COM (2020) p.11

3.1.1.1 Availability of data

More and better data needs to be made available according to the EU Data Strategy. Legal uncertainty regarding what data can be used for and by whom hinders data sharing between businesses in particular, but it is also a problem for public administration. The proposal for a regulation on European data governance,[18] which could manage reuse of data held by private entities in the general interest, is also being investigated as to its possibility of increasing data sharing between private and public entities.

According to the EU Data Strategy, incentives are also needed for companies to share data with each other to a greater extent, and environments are also needed for evaluating various potential initiatives where public and private entities can collaborate on possible solutions that generate value for individuals in their roles as both citizens and consumers.[19]

Significant interoperability issues make it impossible to combine data from different sources within the same sector or between sectors, and efforts are under way to strengthen the European interoperability framework for public services that aim to ensure that collection and processing of data from different sources is done in a standardised and interoperable manner.[20], [21]

Although it is made clear that data from different sources should be shared in the general interest, no legal basis is specified for sharing data between private and public entities that explicitly address the individual's ability to have increased control over this flow of data, because this requires appropriate legislation and clearer political governance.

3.1.1.2 Personal data spaces

The Data Strategy refers to a forthcoming review of the General Data Protection Regulation, which is expected to be able to result in further measures for strengthening trust in the use of data in Europe. Individuals can be allowed to have an influence over their data by means of tools and methods that allow for detailed decisions to be made regarding what is done with the information via

[18] https://data.riksdagen.se/fil/531EF079-826E-49A7-B9EE-05CC816CB8B0
[19] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52020DC0066&from=EN p. 8
[20] https://ec.europa.eu/digital-single-market/en/news/rolling-plan-ict-standardisation.
[21] https://ec.europa.eu/isa2/eif_en.

what the European Commission calls "personal data spaces". An individual's entitlement to data portability is supported by Article 20 of the General Data Protection Regulation and would provide people with greater control over who is able to access and use machine-generated data. This development is predicted to be able to provide significant benefits for private individuals, such as better personal finances, reduced environmental impact, simplified access to public and private services, improved health and more. Standardising interfaces for accessing data in real time and making it obligatory to use machine-readable formats for data from certain products and services are considered essential prerequisites for this.

According to the Data Strategy, the tools must be able to handle consent and applications for managing personal information, and must also make it possible for entities to be able to serve as new neutral intermediaries in the personal data economy. The European Commission believes that such tools have considerable potential and need a supportive environment.

3.1.2 European Blockchain Partnership (EBP)

Since 2018, the EU has been carrying out exploratory development efforts for self-sovereign identity (SSI) and blockchain-based solutions via the EBP initiative, which has 29 participating countries.[22] Through EBP, the European Blockchain Services Infrastructure (EBSI) is being developed, with the vision of utilising blockchains for cross-border digital services as part of European public administration.

Within the scope of EBSI, work is under way on the European Self-Sovereign Identity Framework (ESSIF), which, amongst other things, focuses on cross-border information exchange via SSI using specific standards. These efforts are considered to increase in importance as additional fields of application are investigated for these technical solutions, especially with regards to the enabling of an individual's increased insight and control over their personal data.

3.1.3 Single Digital Gateway, eIDAS and building blocks

It is important that the Single Digital Gateway (SDG) regulation is considered when developing national systems for sharing personal data and making use of

[22] https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership

data that has already been collected, in order for the EU to be able to realise the full potential for the internal market. The SDG involves providing 20 cross-border e-administration services that require public administration to reuse data already provided by citizens and businesses (the Once-Only Principle – OOP). In order to achieve this, standardised data sets, semantics and an infrastructure for cross-border data exchange are needed.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) is one prerequisite in order for the SDG regulation and data exchange (OOP) to be able to work satisfactorily and to strengthen the level of trust in the services offered.

In order to support the digital internal market, the Connecting Europe Facility (CEF) programme is funding an arrangement of generic reusable digital service infrastructures (DSI), also known as common European Building Blocks.[23] These, too, are potentially important for constructing services for increased insight and control over personal data. The building blocks offer basic functions that can be reused in all European projects in order to facilitate the delivery of digital public services across borders and sectors.[24] The objective of the building blocks is to ensure interoperability between IT systems so that private individuals, businesses and administrations can benefit from seamless digital public services wherever they are in Europe.

3.1.4 Legal clarifications needed

During the spring of 2021, the European Commission has been working on an implementing act for the technical system (OOTS – Once-Only Technical System) for an assignment under way (OOP – Once-Only Principle) within the SDG regulation.[25] Member States receive drafts in order for them to be able to provide feedback, and will later vote on the proposal as a committee. By 12 June 2021, the European Commission must adopt the implementing act with its technical and

[23] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+a+Building+Block

[24] See section 4.1 and 4.2 for further information about the development of a common digital infrastructure amongst public authorities and building blocks in Sweden

[25] The term OOP is sometimes used more independently from the SDG regulation in order to describe things like national solutions for a single submission of data, such as Estonia's national solutions based on their X-Road infrastructure instead of the CEF eDelivery building block that is required for complying with information exchange for OOP in accordance with the SDG regulation

operative specifications for the technical system needed for implementing Article 14 (9) of the SDG regulation. In an expert opinion on the first draft of the SDG regulation's implementing regulation for the OOP technical system,[26] the Agency for Digital Government states that it is currently not sufficiently clear whether the legal grounds will be based on transmissions between authorities or via the user. The proposed architectural description and technical specifications for the way that the technical system should work contain uncertainties that are too great. And, according to the expert opinion, the Agency for Digital Government considers that the current proposal for the OOP implementing regulation fails to meet the requirements in Article 14 (9) of the SDG regulation.

In an impact assessment,[27] the Commission states that, by means of the certification review mechanism, users retain their control. This can be interpreted as meaning that the certification goes via the user, whilst previous assessments have indicated that it is a question of an exchange between authorities. According to Swedish law, the answer to this question should be crucial in order to determine the need of regulatory measures regarding, for example, Swedish privacy legislation or registry laws.

Development efforts within the EU and tasks according to the constitution to design contact points for collaboration amongst authorities and other common functions for authorities and businesses have brought with them a number of challenging legal issues. The report by eSam called *Eget utrymme hos en myndighet – en vidareutveckling [An authority's user area – a further development]*[28] considers the development of the user area as a concept. When different authorities can be reached from the same home page, and a user area can be offered by several authorities, such as at verksamt.se, a so-called *common user area* is developed.

The idea is that a single authority should be seen as the owner of the area whilst various authorities provide content and access to the area. The common user area

[26] Memorandum – expert opinion regarding the SDG regulation's implementing regulation for a technical system for automatic cross-border exchange of certification and the application of the Once-Only Principle

[27] A Data Protection Impact Assessment (DPIA) is not a final statement from the European Data Protection Supervisor (EDPS). An opinion from the EDPS that is decisive regarding the implementing regulation for OOP is expected to be made on 12 May 2021.

[28] https://www.esamverka.se/download/18.4472a99d1784abb64fe55a6e/1617090755211/V%C3%A4gledning%20eget%20utrymme%20hos%20myndighet%20210312.pdf

is a portal service where visitors authenticate themselves and, once inside the common user area, rather than seeing different facilities, the user can see only a single common area for the authorities.

The way the common user area is run and managed needs to be consistent with applicable laws, and, according to the report, a number of questions arise regarding who is responsible for what with regards to the area. In addition to this, questions arise regarding which authority should examine a request for an official document or the confidentiality of information stored in the area, and which authority should be responsible according to the legislation that applies for handling cases, data protection and information security. Common areas can generate ambiguities with regards to responsibility between authorities, but also between authorities and an individual using the area who needs to know who to turn to if they wish to exercise their rights according to applicable law. eSam notes that long-term sustainability is promoted when each authority has legal control over its own information assets and is solely responsible for functions that they provide for others.

3.2 The position of the United Nations (UN) on digital ID.

In the review if the UN's various communications regarding insight and control as the terms are defined in this assignment, relevant statements of opinion have mainly involved standpoints on digital identities. In focus is the possibility of using some kind of universal digital ID in order to establish an individual's identity. This would be an example of giving an individual increased control over data about the person's own identity. In the long term, this could result in more people having access to user areas for personal information, personal circumstances and errands with authorities and organisations.

- In 2018, with the support of the UN Refugee Agency (UNHCR), a manifesto was drawn up in which the ability to prove one's identity is equated with a fundamental and universal human right.
- In a digital context, the above means that a global eID system should be developed, which can have consequences for how we store information about ourselves, who has access to that information, and how access is provided.
- Only three percent of developing countries have basic ID schemes where eID can be used for anything more than identification purposes. However, there are no clear measurements of user satisfaction regarding various solutions or what constitutes an eID solution that provides increased insight and control over the user's personal data.

3.2.1 ID as a human right

The US recently adopted A *Human Rights-Based Approach to Data* (HRBAD). This strategy focuses on issues regarding data collection and aims to bring together relevant data stakeholders and develop practices that improve the quality, relevance and use of data and statistics in agreement with international standards and principles for human rights.[29] The strategy is part of Goal 16.9 of the Global Sustainable Development Goals, which involves ensuring the legal identities of all people no later than 2030, including birth registration.[30]

The connection to control over personal data comes from some of the preliminary principles and recommendations formulated in HRBAD, such as data disaggregation. Individuals should be able to freely choose whether they wish to share information, because detailed personal data – especially that collected from marginalised groups – can be used for malicious purposes. HRBAD states that categorising individuals into population groups should be based on self-identification. This requires new tools and digital infrastructures that are not specified but for which some meetings and workshops have been arranged.

3.2.1.1 ID2020 – a digital universal ID

In 2020, the UN organised ID2020, where private companies such as Microsoft and Accenture were gathered together with humanitarian groups, including the World Food Programme and the United Nations Refugee Agency. The common goal is to create digital identities for all people linked to finger prints, dates of birth, medical records, education, travel, bank accounts etc.[31] The focus was primarily on showing possible future solutions rather than building a consensus regarding one specific solution. For example, Accenture demonstrated a prototype app that, amongst other things, uses QR codes to identify individuals.[32] Misgivings about collecting so much information about an individual in one place were considered manageable through solutions based on blockchain technology.

In 2018, the ID2020 alliance manifesto[33] was written in collaboration with the United Nations High Commissioner for Refugees (UNHCR) with ethical

[29] https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf
[30] Goal 16: Peace, Justice and Strong Institutions - the Global Goals (globalamalen.se)
[31] https://id2020.org/digital-identity
[32] https://youtu.be/QYy8a7HDJ0g
[33] https://id2020.org/manifesto

considerations regarding digital ID. It states that the ability to be able to prove one's identity is equated with a universal human right, and that a complement to traditional national identification documents should be developed separately from the control of governing regimes. Individuals should have control over their own digital identities and how data regarding their identities is collected, used and shared, but in order for decentralised digital identities to be recognised and trusted, a consensus is first needed regarding governing principles, design patterns, standards for interoperability and other policy frameworks.

3.2.2 eID and development measurements

Currently, most digital ID systems are linked to specific functions and serve a subset of the population; many are used for the sole purpose of identification. According to the World Bank, just 3 percent of developing countries have basic ID schemes that can be used for accessing a range of online and offline services.[34] 24 percent had no digital ID system at all.

The fact that there are no established tools for measuring the population's satisfaction with eGovernment services is a problem for benchmarking and making performance improvements. Initiatives that have attempted to develop a citizen satisfaction model have lacked a systematic approach.[35] The closest thing to an evaluation of public e-services is the eGovernment Benchmark report, which is based on principles laid out in the eGovernment Action Plan 2016-2020 and the Tallinn Declaration. Eight life events are here used, and they are evaluated every two years. Sweden is considered to be in the highest category of countries with regards to digital public services with human-centric design and digital maturity within public administration, although there are some areas for improvement, such as regarding transparency; that is, the publication of open data.

eID is itself an indicator that is assessed on the basis of whether there is an eID system and if it can be used in other countries. There is no scale for assessing an eID solution itself nor the level of satisfaction amongst the population for national solutions.[36] It is therefore difficult to know what comprises a positive development of eID beyond these factors.

---

[34] World Development Report 2016, pp. 194-195,

[35] https://cordis.europa.eu/article/id/88500-optimising-egovernment-services-for-citizens

[36] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62368

3.3 The OECD's focus on policy relating to insight and control

3.3.1 OECD Digital Government Index (DGI) 2019[37]

- The OECD Digital Government Index generally encourages countries to have clearer governance and training within the public sector and joint production with users.
  - One of the objectives is to increase proactive governance, but it does not mention the possibility of an individual controlling the use and sharing of his or her data as a part of this policy.
  - In the evaluation of the *data-driven public sector* dimension, Sweden is considered to perform poorly, and one clear shortcoming is published open data. However, it is not clear that an open and transparent public sector means increased insight into personal data as defined within the scope of this assignment.

The evaluation is based on how different countries have performed according to dimensions that a completely digital public administration should exhibit. The United Kingdom, Japan and Denmark are highlighted as examples of countries that have been most successful by means of a holistic approach in their respective digitalisation strategies. The index consists of recurring proposals for improved and clearer governance, the importance of the right skills within public administration, and the benefits of including the users of digital services in design processes.

No direct connection is made to the subject of increased insight and control for individuals over personal data and how this should affect a country's ranking in the DGI. The open and transparent public sector dimension does not highlight increased insight into personal data (as defined within the scope of this assignment) as a factor; instead, the focus is on published open data and requirements for standards and interoperability that this entails.

In the evaluation of the *data-driven public sector* dimension, the result is affected by whether citizens and businesses have access to, the possibility of granting approval

[37] OECD Digital Government Index (DGI): 2019 – OECD

for, and the entitlement to refuse data sharing with the public sector and third parties.[38] How this has been achieved according to the way that actual and perceived legal obstacles have been handled on the basis of the GDPR, national legislation or praxis are not analysed. Neither is any comparison made regarding management models and the potential these give for achieving the desired results in a specific manner valued by this index. In some ways, national strategies that seek to centralise the management, storage and sharing of data and that give broad mandates to a national coordinator to govern a common digitalisation policy among public authorities are rewarded.

According to the recommendations, countries performing poorly in this dimension, such as Germany, Chile and Sweden, must adopt a holistic approach for accessing and sharing data, with special emphasis on making use of infrastructures, standards and methods for data sharing that make it possible for organisations within the public sector to make efficient and strategic use of data.[39]

3.4 Observations from the Nordic and other countries

The following seven countries were analysed: Finland, Norway, Denmark, France, the United Kingdom, the United States and India.

The authorities in the Nordic countries have a long tradition of collecting data about individuals, but there are challenges for authorities to develop their management strategies in a digital ecosystem where innovation and data economy are watchwords. Sweden, Finland and Norway have had ambitious goals of being world leaders in developing eGovernment, and Denmark has been especially noted for restructuring its public administration in order to seek to incorporate sustainable development as encouraged by the EU.

The data registers used by the Nordic countries are unique not only in that they have existed for such a long time, but also because they have a legal mandate that allows various authorities to collect and maintain information about the population. Citizens lack an ability to opt out because the systems comprise a key part of the way that the welfare system itself works. In order to keep the system working in accordance with the increasing expectations that citizens have for

[38] Digital Government Index: 2019 results, p. 20 4de9f5bb-en.pdf (oecd-ilibrary.org)
[39] Digital Government Index: 2019 results, p. 30 4de9f5bb-en.pdf (oecd-ilibrary.org)

public services, there is a risk that it be assumed that all eligible citizens understand the consequences, costs, benefits and risks of sharing personal data (or not doing so). Without this assumption, the basis upon which more and more collected data is expected to be used for more effective public services based on data that are shared by consent becomes a problem.

The way that efficiency, legal security, focus on citizens and harmonisation with supra national initiatives are ensured is something characteristic for not only the Nordic countries, but is also a distinguishing mark for all countries when combined with other circumstances, such as the country's digital maturity, the prevailing model of governance, and whether it is a country with a relatively large or small population.

Aspects of the approach used in Finland with regards to providing citizens with increased insight and control over personal data are presented below, after which a summary is given from the external environment monitoring as a whole. For key observations from each separate country, we refer to *Annex 2, External Environment Monitoring*.

3.4.1 Finland

- A markedly high level of ambition for providing individuals with insight and control over personal data and giving the government the ability to make use of that data for creating a proactive public sector with insight into the possible future needs of individuals for public services.
- Insight by means of, for example, portals that collect information and provide user pages is a well-established policy, but there are limits to the amount of control that individuals have over their data; for example, it is not possible to choose not to share data for research.
- The 2019 law regarding the secondary use of healthcare and social data is considered by some to be controversial, since critics are of the opinion that it was not preceded by open debate, and they warn of incompatibility with the GDPR and the use of collected data for purposes other than the reasons for which it was originally collected. Section 24 in particular, which makes exceptions for administrative fines in the event of breaches of the GDPR, is considered problematic.

Finland is often mentioned as a frontrunner with regards to data portability, not least due to the fact that the MyData principles, which have become widespread internationally and are mentioned in the EU Data Strategy, originate in the Finish Open Knowledge Festival, and the fact that the MyData Global headquarters is located in Finland. Finland has distinguished itself by, amongst other things, connecting together public services (such as the Aurora network, an AI-based virtual assistant that guides citizens to public services based on their user data and personal circumstances) or by collecting information in one location (see Soumi.fi below). This allows citizens to experience more seamless flows between different authorities when carrying out errands. The objective is to increasingly enable authorities to act proactively in individual cases in order to generate welfare for individuals and society in general. An example would be by making use of various sources of data to create an individualised health profile.

Suomi.fi is an online service that collects together other services and instructions for citizens and businesses according to life events. Individuals can use the web site to request authorisation (electronic authorisation data is saved in the authorisation register) and check their register data. An individual can use the Suomi.fi register to see data that are saved in registers belonging to certain authorities. Each data processor decides what information is shown, and each register has instructions regarding how an individual can correct or request corrections to inaccurate information.

Something that exemplifies the success of eGovernment in the country is that 50 percent of the population between the ages of 18 and 65, and 37 percent of those over 65, have used *Mina Kanta-sidor*,[40] where citizens can see their own health data and prescriptions. Patients are also able to give or withdraw consent regarding who else can see the patients' health information. Self-generated data from approved healthcare applications can be saved in the data warehouse for a person's own information on the *Mina Kanta-sidor* pages, including current weight, steps and daily activity. All use of the *Kanta* services is recorded in a log, which provides insight into which healthcare organisations have processed a person's data. However, patients are not able to control whether their health data may be used in research.

It appears that the Finish vision is that all information and data can and should be made available via a single platform, where access and connection to different platforms is made as seamless and smooth as possible for the user. In the 2018 government report on the future,[41] digitalisation is considered vital to the creation of a public sector that acts proactively, such as by taking measures for the health development of individuals. However, access to a combination of data about an individual from several different sources is needed for this.

Finland has invested in a comprehensive ecosystem solution involving system integration in order to make data more accessible;[42] however, there are legal uncertainties regarding the secondary use of data. The entitlement to informed

[40] https://www.kanta.fi/sv/web/guest/blogg/-/asset_publisher/1QjC602jKPR6/content/omakannan-kavijamaarat-selvassa-kasvussa

[41] Government Report on the Future, Part 2, Solutions to the transformation of work, p. 42

[42] Aula, V. 2019. Institutions, infrastructures, and data friction–Reforming secondary use of health data in Finland. Big Data & Society, 6(2), 2053951719875980

self-determination and to make decisions regarding one's personal data in accordance with the principles of MyData has not been secured or subject to open public debate. Instead, the choice has been to include an exception for possible violations of the GDPR in the country's own data protection law.[43] The level of ambition and the chosen approach have resulted in some critical voices being raised regarding the compatibility of the vision with, for example, the GDPR and the ability of the future population to make choices and manage their own lives.

3.4.2 Summary of observations from external environment monitoring

It is common for countries included in the external environment monitoring to take life events as the basis for when an individual's insight and control over personal data should be increased, but in some cases, it is simply the parties that are willing to be included in test environments that determine the design and focus areas of the solutions.

Technical solutions, financial means and clear political governance vary between the countries that have been examined, but this is seldom mentioned as an obstacle to the development of a proof of concept or solution. Usually, it is legal interpretations and uncertainties that appear to be the most problematic and that are considered obstacles to development in the area. There are also uncertainties in all countries regarding which incentives and prerequisites (in addition to legal uncertainty) would motivate individuals and trade and industry to demand increased insight and control more actively for individual citizens.

Within project or test environments, the focus is on co-creation between private and public entities, where parts of a model for sharing personal data can be evaluated on the basis of functionality and value creation for the individual. Private entities can participate without first needing to make large investments or evaluate new business models. Components of solutions can be observed in all countries, but no single country has incorporated a holistic ecosystem for sharing personal data between an individual, a public entity and a private entity, where

[43] Big Data & Society, January–June: 1–13, Aaro Tupasela, Karoliina Snell, Heta Tarkkala1 2020 DOI: 10.1177/2053951720907107

both insight and control over personal data are governed personally by the individual.

There are examples of bottom-up initiatives – often inspired by Finland's MyData organisation and its principles – where start-ups and innovative economic associations create various pilot projects in test environments and within regulatory sandboxes. There are also examples of projects initiated by the government, where political will in combination with an opportunity and desire to fund projects generate commitment from several different parties. In most cases, the involvement of the public sector is viewed as necessary on the basis of the involvement of private individuals in these projects, in order to create trust in data-sharing systems and security in the necessary digital infrastructure. In both cases, there is a need for venues in which public and private entities can jointly produce solutions based on clearly identified needs amongst citizens. This may involve part of a life event or, for example, a business opportunity that a company wishes to explore. However, public entities as well as and private individuals and trade and industry need a common understanding of what is meant by data portability and how existing structures, business models and policies are affected by giving individuals insight and control into personal data that is kept by public administration, and consumer and behavioural data kept by businesses and organisations. The transition is complex, and the need of test environments and expertise in designing digital environments can be considered great.

Clear incentives need to be created for all parties in the value chain to use shared data – from the individual to organisations. Individuals need to understand how data can be used and what benefit this can bring for them, such as new services that create value; otherwise, solutions for providing increased insight and control will result only in inactivity and a reduction of shared data. This places high demands on the design and interfaces that affect the user experience, and the generation of commitment in continued use of the services that suppliers of different areas for insight and control can offer.

Companies need to see new possibilities and business models due to their customers controlling more of the interaction between them, otherwise they will not take part in initiatives that attempt to explore the opportunities for increased innovation and value creation. There is also a clear link between the interest of trade and industry to explore new possibilities and the opportunity to fund participation in an experiment or government initiative by means of funds

earmarked for projects within the company's social responsibility strategy. That is, in cases where potential profits cannot be used to engage businesses, there may be an interest in participating if the participation itself can generate goodwill amongst the public and contribute positively to brand development for a certain company or organisation.

4 National circumstances and initiatives

4.1 A common digital infrastructure amongst public authorities is under development

The government commissioned nine authorities to jointly establish a common digital infrastructure amongst public authorities that shall enable an effective and safe exchange of information within and together with the public sector.[44] The purpose of this assignment is to strengthen the ability of the public sector to deliver effective, safe and innovative digital services to private individuals and businesses. The government has also tasked DIGG with analysing the circumstances for municipalities and regions to participate in the common digital infrastructure amongst public authorities for exchanging information.[45]

In its simplest form, the common digital infrastructure amongst public authorities comprises a number of building blocks that together are made up of a number of different standards, frameworks, models, structures and services. Each of the building blocks are beneficial by making other digital development possible. The building blocks are divided into four different categories: *Digital services, Information exchange, Information handling and Trust and security*.[46]

Developing and managing the infrastructure requires structures for governance, and the one responsible for the infrastructure directs the strategic work in consultation and collaboration with other parties. In the interim report regarding the government assignment, we proposed that DIGG should be given overall responsibility for the infrastructure (infrastructure manager).

4.2 The common digital infrastructure amongst public authorities consists of building blocks

This section presents some of the building blocks that are deemed able to create the conditions for increased insight and control over an individual's data kept in

---

[44] The Swedish Government (2019) *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte [Assignment to establish a common digital infrastructure for information exchange amongst public authorities]* Reg. No.: I2019/03306/DF

[45] Regeringen (2020) *Uppdrag att genomföra en analys om förutsättningar för kommuners och regioners deltagande i den förvaltningsgemensamma digitala infrastrukturen [Assignment to conduct an analysis of the prerequisites for participation on the part of municipalities and regions in the common digital infrastructure amongst public authorities],* Reg. No.: I2020/02241/DF

[46] DIGG et al. (2021) *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte [Assignment to establish a common digital infrastructure for information exchange amongst public authorities]*

the public sector and, in the long term, also the private sector. As mentioned above and also noted in the interim report provided in January,[47] as well as the published descriptions of the building blocks,[48] these building blocks are divided into four categories.

4.2.1 Digital services

Digital services refer to building blocks that allow for more efficient development of easily accessible and simple customer interactions. Examples of digital services include *Mina ombud* [My Representatives], *Mina ärenden* [My Cases], *Min profil* [My Profile] and digital post.

4.2.2 Information exchange

Information exchange refers to the building block that creates standardised patterns or common infrastructure services for exchanging information. The category contains the Address Register, API Management and Messaging building blocks.

4.2.3 Information handling

Information handling refers to building blocks that allow for a standardised machine-readable interpretation of properties of information and information services. This category contains the Indexing and Metadata Management building blocks.

4.2.4 Trust and security

Building blocks within the trust and security category contribute to meeting security needs. The category contains the Authorisation, Identity, Traceability, Availability and Trust Rules

4.3 User-centric data ecosystem

Ecosystems and platforms are established terms within both the private and public sectors. They are used to describe the collaboration and use of common resources and the dependencies that arise in the ecosystem or platform.

---

[47] DIGG et al. (2021) *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte [Assignment to establish a common digital infrastructure for information exchange amongst public authorities]*

[48] https://www.digg.se/utveckling-av-digital-forvaltning/digital-infrastruktur/samverkansaktor#rapporter_och_redovisningar

4.3.1 Digital ecosystems in general

In order for public administration and businesses to be able to succeed in developing more cohesive, user-centric and seamless services based on life events, there is a great need for taking a holistic approach. This means that technical, legal, semantic and organisational prerequisites need to be seen as a whole – an ecosystem.

A digital ecosystem is a defined technological environment consisting of infrastructure, digital equipment, digital resources (services, applications and software) and users who collaborate with one another. Digital ecosystems often adopt principles from natural ecosystems. Within digital ecosystems, interested parties can interact in order to generate value for their users/customers, themselves, and, in the long term, also each other.

Unlike biological ecosystems, digital ones often have a single key player that initiated the ecosystem, and other parties that have joined it can make use of the infrastructure in order to generate value. The key player is referred to in different ways depending on the responsibility, type of ecosystem etc., but it is commonly clear that this party is responsible for the ecosystem.

Digital ecosystems are often separated from the external environment by agreed rules for how systems within the ecosystem should work together and communicate with one another. This interoperability can take place organically in a decentralised manner (cf. the way the internet is constructed) or controlled from the top down by one party.

There is often a market linked to a digital ecosystem where the platform leader and third-party developers come to an agreement and are able to offer their respective products and services together or separately.

4.3.2 Different types of digital ecosystem

Business ecosystems consist of networks of different parties such as companies, research centres and public entities that collaborate across sector boundaries. The AppStore and PlayStore are two examples of business ecosystems where third-party developers offer their applications based on the underlying iOS or Android platforms. The platform leaders, Apple and Google, determine the rules for, e.g., who is permitted to sell and distribute their applications, what requirements must be met, and what percentage must be paid from a completed transaction.

In a *data ecosystem*, the focus is instead on the data that is shared and how it flows between the parties within the ecosystem.[49] There is often a platform, an infrastructure, where data is shared using APIs.[50] The parties may consist of individuals as well as organisations. One example of a data ecosystem is DIGG's data portal for open data. The objective of the portal is to improve Sweden's ability to make use of data as a strategic resource and improve digital collaboration between the public sector, trade and industry and civil society.[51]

4.3.3 Management and ownership of data ecosystems

Digital ecosystems are managed by distributing rights and responsibility amongst the parties in the ecosystem and through necessary rules and processes.[52] The management structure is normally determined by one party that takes on the role as platform leader and that accordingly makes decisions and maintains the platform. The leader often has overall responsibility for the infrastructure and for ensuring that only entities and services that meet certain requirements are allowed to be affiliated and that these comply with the requirements and commitments that have been set.

In addition to the platform leader, an ecosystem can also be influenced by other entities in various ways. This could be the owners themselves, formal or informal partners, producers of important data sets, organisations that have large user bases, and organisations and individuals that are actively engaged in the ecosystem. Additionally, an ecosystem needs to comply with current laws; that is, the legislative provisions that are applicable where the ecosystem will be operating. This includes the EU General Data Protection Regulation and any associated national regulations if the ecosystem will be processing personal information.

An ecosystem's platform may have one or more owners and different constellations.

Sole public ownership means that a public entity, usually an authority, is the exclusive owner or constitutes the platform leader. One example of such a

[49] Lindman et al., 2015
[50] Linåker & Runeson, 2020
[51] https://www.digg.se/om-oss/nyheter/2020/digg-lanserar-sveriges-nya-dataportal
[52] Alves et al., 2017

platform is the Swedish Public Employment Service's *JobTech Dev ecosystem*, in which external service providers can use data from *Platsbanken* to offer digital services for improving job matching for job seekers.

Joint public ownership means that two or more public entities act as owners or serve as platform owners as a consortium. One example of such a constellation is HSL Developer Community, which is a data ecosystem focused on public transport within the Helsinki region of Finland. Platform leader HSL/HRT is a company jointly owned by the municipalities within the region.

Joint public-private ownership is when two or more public and private (or civil society) entities own or serve as platform owners as a consortium. One example of this is *Trafiklab*, which is a data ecosystem for Swedish public transport. The platform leader is *Samtrafiken*, which is the business jointly owned by the regional public transport companies together with private operators.

As for sole private ownership, the AppStore and PlayStore platforms are concrete examples.

4.3.4 The MyData example

MyData Global is an interest organisation that, amongst other things, aims to strengthen the empowerment of individuals in relation to data about themselves, improve people's ability to make well-informed decisions, and work more consciously and effectively with organisations that create or use an individual's personal data. In Sweden, the term MinaData is used to describe MyData.

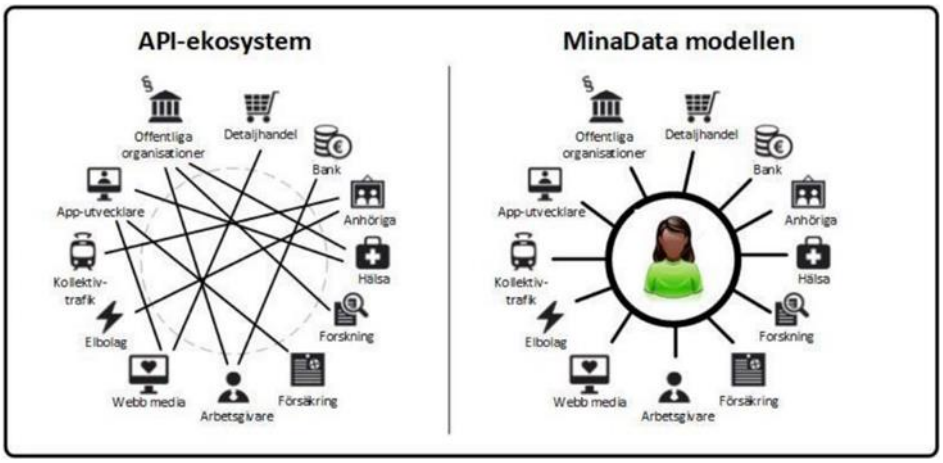
MyData Global has developed the following principles for designing user-centric data ecosystems:

- Individuals must have a complete understanding of and insight into policies, agreements and how their data are used.
- Individuals must have the power to give, refuse or withdraw their consent to the sharing of data.
- Individuals in focus when services need data from each other.
- Individuals must be able to safely manage their personal information in the manner they prefer.
- Data portability between services and storage areas must be promoted.
- Interoperability must be promoted so that all personal information is transferable and reusable without individuals losing control.

4.3.5 The eSam model for user-centric information management

In a report from 2020, *eSam* developed a model for user-centric information management inspired by the principles behind MyData. Amongst other things, this included the fact that data about people is a resource that the individuals themselves should have access to and control over.[53]

Figure 1. The MyData-model



The *eSam* model was developed in order to complement the current more API-based ecosystem by basing it on the individual's need to handle various life events and entitlements related to data about themselves. The purpose of the *eSam* model is to strengthen the role of the individual in the digital flow of information between public organisations, and to increase the amount of control given to individuals over how their personal information is processed.

One key component of the *eSam* model is a so-called "MyData account", which is intended to provide individuals with the ability to see relevant data, view how consent is managed, and other important features. According to *eSam*, such a model would allow individuals to easily approve various data flows between organisations.

[53] https://www.esamverka.se/download/18.1d126bc174ad1e6c39b6a9/1600695706378/eSam%20-%20MinaData%20v1.0.pdf

4.3.6 The Solid example

Solid (Social Linked Data) is a project with the aim of decentralising the web and giving control of personal information to individuals.[54] Solid wishes to create an effective location for individuals to manage their data and personally influence how and where information is stored, which people and organisations have access to specific information, and how data should be shared.[55]

The individual saves and stores information in personal online data warehouses, also called PODs, and the individual personally determines where PODs should be stored. The individual can move his or her information between several PODs and decide which applications are allowed to access each respective POD. Applications that wish to retrieve information from PODs must first be authenticated by Solid. By deciding which information is to be stored in each POD, where each POD is stored, and which applications are authorised to use the data, individuals are given complete control over their information.

Figure 2. Personal online data warehouse[56]

PODs protect data by means of access control rules. These rules can be configured in such a way that individuals can personally set time limits etc.

[54] The project was initiated by Tim Berners-Lee, who is known for inventing the World Wide Web together with the Massachusetts Institute of Technology (MIT).
[55] https://solidproject.org
[56] Image from https://solidproject.org

Individuals interact with the system either through a domain-specific application or a web browser. The application can ask the individual for consent for using some of the person's data in order to provide the individual with something of value.

4.3.7 Important characteristics for user-centric data ecosystems

There are certain characteristics for user-centric data ecosystems that are fundamentally important to include in the continuing work. Amongst other things, the data ecosystem must:

- meet the needs of individuals regarding control and insight,
- enable individuals to personally store information in their own chosen place in the ecosystem,
- have an entity responsible for the ecosystem,
- have a functioning infrastructure that bridges interoperability issues as a basis for data sharing,
- have a clear framework for roles, responsibility, approaches and authorisation for the various features of the ecosystem.

4.4 Insight and control in certain public services

For some time, there have been various initiatives aiming to provide increased insight and, to a certain extent, control. The implementations are done together by the public and private sectors. We choose to highlight these three as examples of different sectors developing solutions in the area in various ways.

4.4.1 Journalen på nätet

The *Journalen på nätet [Patient records online]* e-service available on 1177.se gives individuals older than 15 years of age the ability to read parts of their patient records. Inera AB provides and is responsible for the service, which is used by more than four million people.

Journalen på nätet allows individuals to see what information the healthcare services have about them in order to get patients more involved in their care and health. Patients respond positively to being able to read their patient records online and to the possibilities that this resource allows. Those who use *Journalen på nätet* value their opportunity to access test results, have an overview of their health

and interactions with the healthcare services, and the possibility of following up planning and medical care after their visit.[57]

Regions, municipalities and private healthcare providers that are publicly funded can join *Journalen på nätet*. The service contains things such as information about record entries, appointments, medical prescriptions and test results.

The details shown vary between regions, but no region shows all of the information contained in the patient records to private individuals. Each healthcare provider also chooses what information from their system should be made visible to the individual, which results in variation even within regions.

Individuals have direct access to details in their patient records, but there is currently no way for them to download or forward information to other parties. Additionally, individuals also have the ability to seal – that is, remove the possibility of direct access – their own access to all or parts of *Journalen på nätet*. Individuals can do this themselves or request the healthcare services to do it for them. Sealing *Journalen på nätet* can also be initiated by the healthcare services if it is assessed that the information is harmful to the individual, healthcare staff or third parties.

In 2017, the Supreme Administrative Court (HFD) found that the Patient Data Act (2008:355) only permits patients themselves to have direct access to their records.[58] Accordingly, the ability to allow a representative to have direct access to information from patient records was discontinued.

Individuals may request information about when medical staff have read their patient records. In some regions, it is possible to view excerpts from the log directly in the *Journalen på nätet* e-service, whilst special arrangements are needed in other regions.

4.4.2 minPension

Everyone who has earned towards a pension in Sweden can log in to *minPension [My Pension]*, see their entire pension and make pension projections. The service is run and funded half by the government and half by the pension providers. This

[57] Moll, J., et al., (2018). Patients' Experiences of Accessing Their Electronic Health Records: National Patient Survey in Sweden. *Journal of Medical Internet Research*; 20 (11) 2018.
[58] HFD 2017 ref 67.

makes *minPension* a neutral and independent web portal that is free of charge to the user. More than 30 entities within the pension sector provide information to *minPension*.

minPension processes personal data in order to perform a task of general interest in collaboration with the government – via the Swedish Pensions Agency – and the insurance industry – by means of Insurance Sweden and the affiliated pension entities that provide pension information to minPension.

The Swedish Pensions Agency is assigned to provide pension savers an overview of their entire pension based on the needs of the individual. The assignment is performed voluntarily by means of this collaboration. Amongst other things, *minPension* is tasked with providing everyone who earns a pension in Sweden with a general picture of their pensions, a projection for future pensions, and information about what affects pensions and the importance of an occupational pension and private pension savings. *minPension* retrieves information from the government as well as the insurance industry.

minPension is thus an excellent example of collaboration between the private and public sectors, and it provides citizens with greater insight into the information upon which future pensions are based.

4.4.3 Digital Post

DIGG is responsible for the infrastructure for digital post from public entities called *Mina meddelanden [My Messages].* DIGG is also one of four entities that provide a digital post box. Joining *Mina meddelanden* means that a person agrees to receive digital post from public entities that have also joined the service or that will join it in the future. It is possible for an individual to decide if they do not wish to receive digital post from certain senders.

Förmedlingsadressregistret [the Address Forwarding Register] (FaR) is the basis of the infrastructure for digital post. The register contains information about everyone who is in some way connected to the infrastructure. This includes recipients, public entities who are sending post, distributors and post box operators. When the recipient acquires a digital post box, they are registered in FaR and a profile is created. The profile that is created during registration contains the recipient's Swedish personal identity number and the individual's choice of post box operator. The profile also contains information about how the recipient wishes to receive messages.

Messages that are stored in a digital post box cannot be requested as official documents because the digital post box should be considered as the post box holder's personal user area.

A user area[59] is a legal concept that has formed the basis of a legal model solution in the eDelegation's guide for developing operations within eGovernment and is applied to the government *Min myndighetspost [My post from authorities]* post box.

4.5 Examples of user-centric data ecosystems

4.5.1 Hälsa för mig [Health for me]

Hälsa för mig was a government initiative started in 2012 that was included as part of the main commission of the Swedish eHealth Agency (previously *Apotekens Service Aktiebolag*). The service would contain a place – a user area – at the Swedish eHealth Agency for storing information, also called a *hälsokonto [health account]*, that would make it possible for individuals to collect, get an overview of and share their health information. The personal health account would be free of charge, and the aim of the initiative was to strengthen the involvement of individuals in their own health and to give them the right and ability to exercise control over their own health data. The personal health account would give private individuals in Sweden the possibility to save, manage and share their health data throughout their lives.

Hälsa för mig would consist of a platform upon which businesses and organisations could build innovative health-related services for private individuals in the form of applications. People would be able to use their personal health accounts to decide for themselves what information would be saved and shared with other parties, and to ensure the accuracy and quality of the information. Information from the health account would only be made available to others – apart from the individual personally – after the person had granted their express consent. This would be possible by means of a consent feature built into the service. If an application were to be linked to the health account and the individual had given express consent to his or her information being shared, the recipient of that personal data (i.e., the application provider) would be responsible for the continued use of the information in the application.

[59] For more information about the legal perspective of user areas, see Annex 3, Chapter 4 on user areas

In its agreement with application providers, the Swedish eHealth Agency would set requirements that personal information could be used only in accordance with the current data protection legislation, and that consent would be required each time information was to be disclosed.

Using the infrastructure that the Swedish eHealth Agency was supposed to provide, an API-based ecosystem would have been created so that both public and private organisations would be able to offer services over which the individual would have control and be in the centre.

Following judicial review, the Swedish Data Inspection Board,[60] and later the Administrative Court,[61] did not approve the Swedish eHealth Agency's interpretation of the legal bases for carrying out the assignment.

In its review, the Swedish Data Inspection Board found that the *Hälsa för mig* health account did not meet the requirements of the data protection legislation and therefore issued a number of injunctions. The Swedish eHealth Agency appealed against the decision to the Administrative Court of Stockholm, which in turn rejected the appeal.

In its ruling, the Administrative Court of Stockholm assessed that controllership of the health account fell on the Swedish eHealth Agency, since it was the entity that determined the outer framework for processing personal data and, in the long term, the purposes and means of processing operations. The court found that this was not a case of a so-called user area as offered by some authorities as a sort of digital storage area for individual users. The Administrative Court also found that, although individual users of the service would retrieve information and share data, it was only the Swedish eHealth Agency and its personal data processors that would manage data collection as a whole. According to the Administrative Court, the fact that registered users would have considerable influence over the service and that information was to be retrieved from other data controllers did not reduce or limit the controllership of the Swedish eHealth Agency. Neither did the

[60] Supervision according to the Personal Data Act (1998:204) – the Swedish eHealth Agency's *Hälsa För Mig* service, 2017-04-21, Reg. No.: 2276-2016.

[61] Administrative Court of Stockholm, judgement of 2018-05-24, Case No. 11458-17.

fact that data subjects would have given their consent to having their information processed mean an end to the responsibility of the data controller.

Following the verdict of the Administrative Court, the Swedish eHealth Agency assessed that legal support for the health account was insufficient, so the authority chose to not appeal against the judgement, ending that work.

4.6 Summary conclusion

Individual services as described above are good examples that can be considered ecosystems based on collaboration between the private and public sectors.

Digital post, *minPension*, and *Journalen på nätet* all focus on improving an individual's ability to have insight. The fourth example – *Hälsa för mig* – aimed to go further than merely giving insight by also providing individuals with control over their information and the possibility of sharing data with other parties. There are considerable challenges – especially legal ones – in providing individuals with control over their information, not least of which in relation to public entities, as shown by experiences from the *Hälsa för mig* example.

The services are largely sector-specific solutions, but there are experiences from all of the above services where issues concerning collaboration between the public and private sectors, business interests, funding, legal questions, development and administration are all of interest for further efforts in developing individual solutions for insight and control.

5 Technical Proof of Concept

The Swedish Public Employment Service was tasked to lead the technical work and development of the technical PoC mentioned in this commission from the government.

The activities of the Swedish Public Employment Service ultimately aim to effectively bring together employers looking for manpower and job seekers looking for work, to prioritise and equip those who are far from the labour market, and to contribute to permanently increasing employment in the long term.

Development today is moving quickly in several areas, and technical innovations cause changes and developments also in the labour market. In developing this PoC, we have assumed that customers have a desire to personally be able to act – to take control over their situation. The job seeker wants to find work, and the employer wishes to find the right worker.

The proposed technical PoC is based on the current situation and explores the present prerequisites and possibilities.

5.1 Life event: starting work

Starting with a life event involves identifying needs amongst citizens for which the public sector is there to meet, regardless of the responsible authority/organisation. A life event describes something that occurs in a person's life that involves a change in their personal circumstances that may involve a digital or analogue encounter with the public sector. The starting work life event is very complex, and there are a considerable number of activities, interventions, and relations with authorities and other entities. The target group that are facing unemployment and a job seeker are differentiated and require different types of interaction according to personal circumstances. In working with the proof of concept, the Swedish Public Employment Service has chosen to focus on a limited part of this life event that involves looking for work.

5.2 Description of Proof of Concept (PoC)

From the outset, the aim has been to expand the Swedish Public Employment Service's *Min profil [My Profile]* e-service with new functionality in relation to existing legislation and applicable law within the scope of the commission from the government.

The aim of the proof of concept is to show how the ability of an individual to have insight and control over their data kept in the public – and in the long-term, also the private – sector can provide clear added value for the individual. Privacy and personal retrieval and sharing has been at the core of the PoC development, and thus have also been the legal conditions for processing and sharing personal data.[62] The PoC shows how an individual can retrieve data from a few selected authorities and organisations in order to be able to create a CV at the Swedish Public Employment Service with validated information/data from validated sources, which can then be used to facilitate a job search.

The PoC provided is not a finished system that is ready for deployment. The PoC that has been developed should be viewed as an exploratory test implementation. The implementation[63] is a CV service that is integrated with a limited number of authorities and entities.

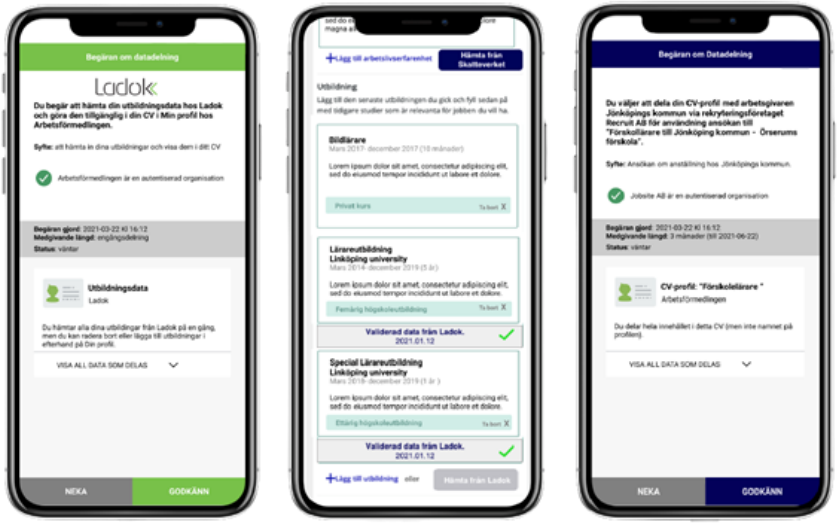
Brief description of the chosen scenario: *Anna is looking for a job as a preschool teacher and shares her CV from the Swedish Public Employment Service with many job search websites. Her CV contains validated data from different authorities, including her driving licence, registered address and educational certificates.*

The aim of this proposed solution is for Anna to be able to use it to request/retrieve validated information from authorities that she needs when looking for a job, and for her to be better able to transfer information between entities in different contexts. This makes the information more credible to readers and allows Anna to be able to streamline her application process.

[62] See Annex 3, *Comprehensive legal analysis of the possibility of increasing insight and control for individuals*

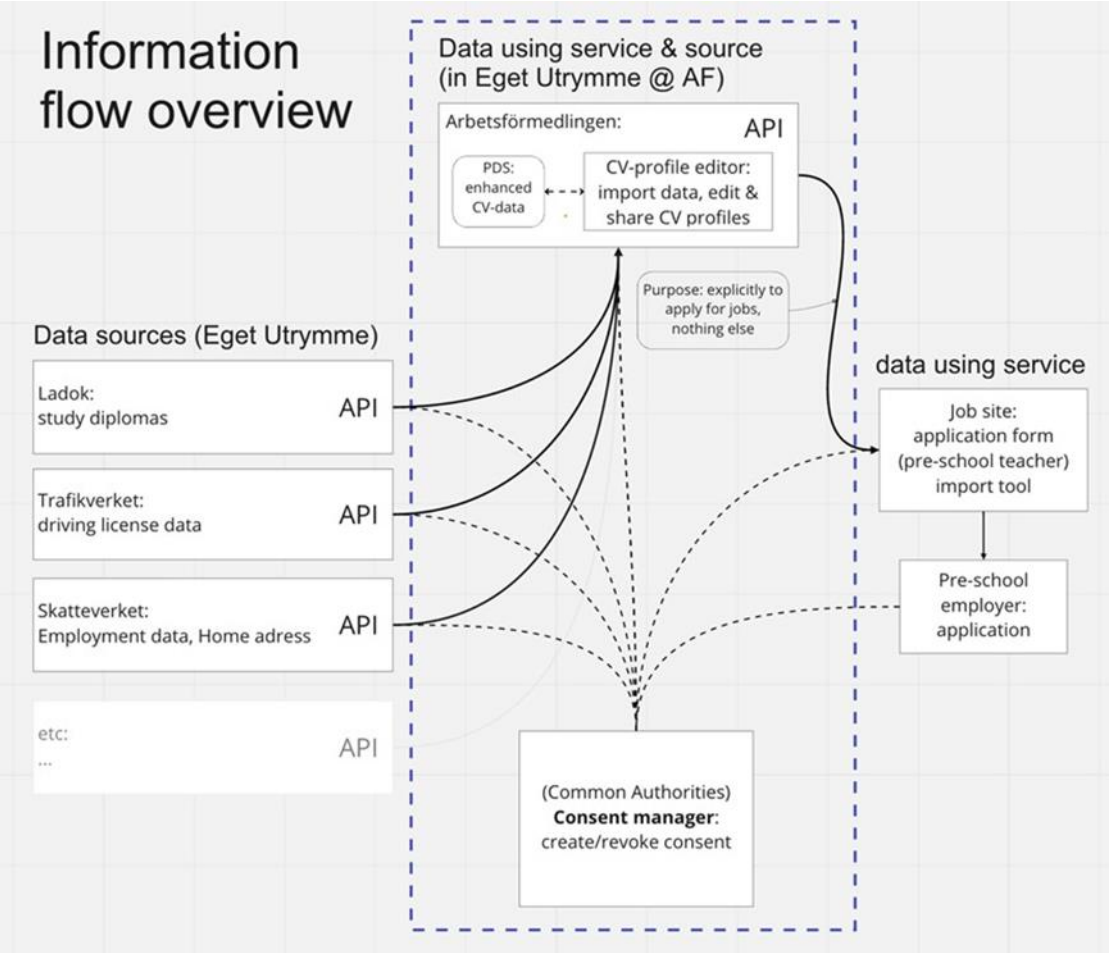
[63] As part of this assignment, we have not produced a general model for security and privacy issues, such as how a general operator should process and define which third party services are reliable for sharing data with.

Figure 3. Images showing the application process



This transmission of data that occurs within the framework of the PoC (from identified authorities – see picture) upon request of the individual (Anna) to a user area can be considered consistent with applicable law as long as the information in relation to the individual is not classified as secret, and as long as an electronic transfer may and can be done securely. According to applicable legislation, the model must therefore require that an individual take a certain measure considered to correspond to a request before the information is shown or transmitted

Figure 4. Information flow in the proof of concept



5.3 Information and IT security

There are significant legal requirements that must be met in order for information to be exchanged between authorities, municipalities, independent parties, county councils/regions, employers etc.

In this technical PoC, the Swedish Public Employment Service has worked systematically with information and IT security in order to ensure that both individuals and the information that is processed are adequately protected and that governing statutes and legal frameworks are complied with.

By definition, information security includes confidentiality, accuracy, accessibility and traceability of the information, but also involves responsibility, risk awareness and having a comprehensive view. It is a complex area and, in addition to solutions for technological security, it also involves security-related solutions with

regards to, for example, administrative and personal security. Additionally, there are of course financial and legal aspects to take into account.

Since we today live in an information society in which greater quantities of data than ever before are processed, stored, communicated and duplicated, information security must be considered a prerequisite in order for phenomena in society to be able to work in a secure manner. The importance of citizens and businesses feeling that they can trust the authorities' way of processing information must therefore be emphasised.

The Swedish Public Employment Service's work on this PoC has touched on the following areas related to information and IT security.

The purpose and entitlement with which information is exchanged: Who is entitled to access what information, and in what way?

Managing information on behalf of others: A digital infrastructure in which authorities and other entities collaborate by using the same technological components may lead to an authority managing information for others. Such management involves both processing, storage and delivery; that is, management of a more long-term nature or on a temporary basis.

Public access and secrecy when information is exchanged: Information stored by an authority is covered by, amongst other things, the provisions of the Public Access to Information and Secrecy Act (2009:400), meaning that an authority is obligated to protect information that is classified as secret. This means that it is not to communicate or disclose information that the legislator intends to protect to any unauthorised individual or entity.

Controllership when information is exchanged: The choice of data controller and personal data processor must be established when personal information is processed in the architecture.

Specific information and IT-related requirements when testing this PoC are presented in Annex 5, *In-depth description of the proof of concept.*

5.4 Legal prerequisites for the PoC:

The legal prerequisites for the e-service are essentially as described in the general legal description found in Annex 4, *General legal analysis of the possibility to increase insight and control for individuals.*

The structure of the PoC is based on the following:

- The individual has a User Area [*Eget Utrymme*] with the authorities that are relevant to this PoC.
- The authority has controllership for the content, even though it is not entitled to read what is contained in the user area, and this limits the way in which the area may be used and the way that information is shared with third parties.
- The individual can personally process and add information in their user area.
- Only authorities can provide user areas (in accordance with the prerequisites for only technical processing and storage in Chapter 2, Section 13 of the Freedom of the Press Act.) It is possible for this to be outsourced, but the third party then serves as an extended arm of the authority.
- Only the individual has access to the content. The authority may not access the content. As an authority, we may only access operational and security information.

5.4.1 My Profile is expanded with new functionality

As previously mentioned, the aim from the outset has been to expand the Swedish Public Employment Service's *Min profil [My Profile]* e-service with new functionality in relation to existing legislation and applicable law.

The new functionality of My Profile aims to offer a service, which is completely optional, for individuals who are looking for work so that they can effectively design a CV that contains the producer's data that they have retrieved themselves. It must also be possible for individuals to share their completed CVs with employers or recruitment agencies. These are henceforth referred to as third parties. It should also be possible to send the CV to the Swedish Public Employment Service's reception point[64] in order for an item[65] to be initiated in accordance with the Administrative Procedure Act. These procedures will henceforth be termed the *new functionality*.

In accordance with the EU General Data Protection Regulation,[66] no sensitive personal information or data warranting special protection according to the

[64] A function at the Swedish Public Employment Service where electronic documents are received, registered on arrival, recorded and in some cases acknowledged.
[65] There is no visualisation of this in the PoC.
[66] Article 9 of the EU General Data Protection Regulation.

Swedish Public Employment Service's data registry laws will be processed within the scope of the new functionality.

5.4.2 User area

Individuals are given access to the new functionality via a so-called user area. This means that the Swedish Public Employment Service provides the service only as a part of the technical processing and storage done on behalf of others.[67] A user area can be described as a confidential electronic location that only the user has access to.

5.4.3 Legality

An authority may take measures only if these are supported by the legal system.[68] Legal support is thus needed in order for the Swedish Public Employment Service to be able to offer this functionality. When assessing the impact of the principle of legality on the Swedish Public Employment Service's possibilities of providing the new functionality in question, the purpose of the service must be linked to the commission given to the Swedish Public Employment Service.

In the instructions given to the Swedish Public Employment Service, it is stated that the authority should work to improve the way the labour market works by effectively bringing together those looking for work with those looking for workers.[69] The budget and policy specification for 2021[70] states that, in the preparatory work in advance of the forthcoming reform of the Swedish Public Employment Service, the authority must especially develop the digital infrastructure needed for facilitating an effective exchange of information between relevant parties active on the labour market. An e-service that aims to support individuals in producing a CV that contains data from the producer, with the possibility of sharing it with third parties, can therefore be considered to fit within the authority's commission. In the long term, the effectiveness of the labour market will increase due to quicker recruitment processes.

---

[67] According to Chapter 2, Section 13 of the Freedom of the Press Act (1949:105).

[68] SOU 2018:25, p. 280.

[69] Section 2 of Ordinance (2007:1030) with instructions for the Swedish Public Employment Service. The Swedish Public Employment Service must promote improvements to the way that the labour market works by, 1) effectively bringing together job seekers and employers searching for workers.

[70] https://www.esv.se/statsliggaren/regleringsbrev/?rbid=21825

5.4.4 Processes that occur in the new functionality

- Personal retrieval initiated by the individual for starting on the CV.
- The possibility of editing the parts of the CV that are not validated.
- Personal sharing initiated by the individual when the CV is ready.

5.4.5 Controllership

In view of the fact that controllership of the user area has never been examined by a higher court, it is not easy to determine which party has controllership of the information that is processed. According to common practice that has developed regarding other digital services, it may be possible to clarify the current legal situation. With regards to the processing of personal data that occurs within the authority's enterprise system, which is separate from the user area, it is relatively straightforward to establish that the authority is the controller. In such cases, it is the authority that determines the objective and means for processing personal data.

In the absence of common practice clarifying the situation, there are some difficulties in ascertaining where the role of controller should be assigned with regards to digital services providing a user area. It has also become clear that there is a lack of clear guidelines to help authorities assess where to assign the role of controller.[71]

According to the EU General Data Protection Regulation, the one who – alone or together with others – determines the objective and the means for processing personal information is controller for that procedure.[72] In Sweden, the controllership of authorities is also often regulated by a records statute that controls the relevant area in which the authority processes personal data. According to Section 3 of the Swedish act regarding processing personal data in labour market activities, lag (2002:546) *om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten* (AF-PuL), the Swedish Public Employment Service is controller with regards the processing done by the agency.

There is much to suggest that it is the authority that sets up a digital service with a user area that determines the objective and means for processing personal data in the user area. This responsibility should cover both the content itself as well as

[71] SOU 2018:25 p. 288
[72] Article 4.7 of the General Data Protection Regulation

personal information related to the operation and security of the user area. In our opinion, such an understanding finds the support of the judgement of the Supreme Administrative Court, HFD 2012 ref. 21. The case expresses a holistic view of controllership, which in principle necessitates a far-reaching responsibility. In this case, it was not the data controllers that had created the technical means; instead, the controller had merely referred to certain technical services. However, this did not prevent the court from considering the Swedish Social Insurance Agency to be data controller.

As regards the circumstances surrounding the user area, the authority has in these cases not only taken the initiative to processing personal data but has also created the technical prerequisites for the service. This indicates even more strongly that the authority is sole controller with regards to personal data in the user area.

In view of the fact that the General Data Protection Regulation has recently come into force, established practice and legal literature in the area are scanty. As regards Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive), which is the predecessor to the General Data Protection Regulation, the definition of data controller is almost identical to Article 4 (7) of the General Data Protection Regulation. This also applies to the PuL that has been incorporated into Swedish law on the basis of the General Data Protection Regulation.[73] Such similarities can also be found in other parts of the General Data Protection Regulation, such as the definition of personal data and the processing of such data. This means that previous decisions from Swedish courts will be taken into account. We consider it unlikely that a Swedish court or the European Court of Justice would drastically change the praxis that has developed.

In the new functionality, the Swedish Public Employment Service determines the purpose for processing personal data; that is, the possibility of creating a CV that contains data from a validated source. The Swedish Public Employment Service has also determined the means by which personal data are processed by allocating the technical transmission capabilities offered for personal retrieval and sharing. Additionally, it is the Swedish Public Employment Service that determines that

[73] See the Data Protection Directive, Article 2 (a) and Section 3 of the Personal Data Act (1998:204)

this functionality will be set up within the scope of the user area as well as how it will be designed, what security levels will apply, what options will be available for collecting and providing information, and who it is that shall be responsible for operation and administration. It is also the Swedish Public Employment Service that sets requirements for using the user area, and it is the same agency that is able to satisfy the rights belonging to individuals.

The Swedish Public Employment Service is data controller both for the retrieval of data (transmission) that occurs as well as the sharing of information that takes place until the data are received by an external party, since it is the Swedish Public Employment Service that provides the purpose and the means for these transmissions, notwithstanding the fact that this processing occurs before the data are received by the authority (if applicable).

Controllership brings with it obligations for the one responsible, such as the responsibility to provide information to data subjects, protect the data from unauthorised access, and ensure that no more information than necessary is processed and that such processing does not continue for longer than needed. The data controller must also respect the rights of data subjects, such as the entitlement to have corrections made, to have information deleted, to receive details about what information is stored via a so-called extract from the register etc. Additionally, data subjects are entitled to compensation if they have suffered material or immaterial damage as a result of a violation of the General Data Protection Regulation in which the data controller was involved.

An example could be if the technical design results in personal data being stored for longer than warranted and an individual suffers damage as a result.

All rights belonging to users of the new functionality must also be able to be met by the controller without the authority itself having access to the user area in order to maintain the status of the user area.

5.4.5.1 Scope of controllership

As shown above, controllership brings a number of obligations that the data controller must comply with. The question is whether the authority is able to do so. In the following section, we will give a general account of the problems associated with controllership in relation to the way a digital service with a user area is set up.

There is a possibility that documents in the user area are not considered to be public if the documents are stored only as a step of the technical processing operation or technical storage on behalf of others. However, this assumes that digital services with a user area are given a special design. For example, the content must be separated from the authority's IT environment, at least logically from the authority's enterprise system. Additionally, staff working at the authority should not as a rule have access to information in the user area. The information must therefore be reserved for the user.

With this in mind, there is no guarantee that the authority can check that personal data are processed in a manner that is in agreement with the General Data Protection Regulation. The *Digitaliseringsrättsutredningen [Digitalisation Law Inquiry]*, for example, questioned how an authority can ensure that private individuals only enter adequate and relevant personal data in relation to the purpose for processing that data.[74]

The user area is designed so that staff at the authority should not have access to the information stored there; only in exceptional cases should such access be possible. The data controller is also obligated to provide an extract from the register on the request of the data subject, as set out in Article 15 of the General Data Protection Regulation. The extract from the register must contain information about the processing operations that the data controller conducts using the personal data. Amongst other things, the purpose for which the personal information is processed must be stated. Additionally, according to Articles 16 and 17 of the General Data Protection Regulation, the data controller must in some situations delete or correct personal data upon the request of the data subject.

The above obligations show that an authority serving as data controller must establish technical and organisational procedures in order to comply with the General Data Protection Regulation. These procedures are extensive in nature, and the question is whether the authority needs to have access to the information in the user area in order to be able to carry out its responsibility.

For the data controller, a number of obligations arise towards the data subject. For example, personal data may only be processed for a particular purpose, and

[74] SOU 2018:25 p. 290

personal data must in such cases be deleted and corrected upon the request of the data subject. As a result of this, it may well be asked whether the exception in Chapter 2, Section 13 of the Freedom of the Press Act can possibly be applied, since the obligations according to the General Data Protection Regulation are so far reaching. One prerequisite in order for the user area to be able to fulfil its function is that documents stored there remain the property of the user and cannot be accessed by others.

In order for an authority to be able to completely ensure that personal information is processed in the user area only for a certain purpose, it may well be necessary for the authority to have a certain level of access. In that case, there is a disagreement between the prerequisites for the user area and the obligations that come with controllership, which in that case means that there is a potential conflict between the EU General Data Protection Regulation with the foundation of the user area. If, however, by setting technical limitations and clear terms of use, the authority succeeds in counteracting misuse and thus ensures that only the information needed for the purpose is processed, this conflict should not arise.

That is the goal we have with this PoC, and in that vein, as far as possible, preselected alternative answers must be used, and to the extent that free text fields are necessary to meet the purpose, it must be clear to the individual what the field will be used for, which could be clarified in the terms of use. There must be technical limitations in place so that individuals do not write information that is inadequate, non-relevant or not permitted. The Swedish Public Employment Service prevents this through clear guidelines (terms of use) regarding what may be written in free text fields and by establishing technical limitations (spam filter, limitations to the size of uploads and formats). If inadequate and irrelevant data are nevertheless entered, they must be immediately removed.

By actively working according to privacy by design, the authority knows what de facto processing occurs in the user area without needing to access the content. Additionally, the Swedish Public Employment Service may have access to operational and security information, which includes meta-information. The authority can thereby detect some misuse without needing to access the content.

Of course, the Swedish Public Employment Service could avoid many of the obligations stipulated in the General Data Protection Regulation if it were instead the user who was considered to be the data controller for content in the user area. There yet remains some uncertainty regarding the assigning of controllership, and using a sympathetic interpretation, perhaps the user can be viewed as data controller in individual cases. However, in our opinion, there is reason to find fault with such an interpretation.

5.4.6 Coordinated processing

The Swedish Public Employment Service's controllership ends when an individual's data reaches the application form of a third party. The third party becomes data controller when the information reaches the application form, and does not process any personal data in the new functionality. This is therefore a case of transmitting data on behalf of one party (the Swedish Public Employment Service) to another (third party), which is termed coordinated processing. The same also applies if sharing is done on the initiative of the individual. With coordinated processing, there is no requirement for arrangements to be made between the parties, as is the case with joint controllership (Article 26 of the General Data Protection Regulation), a so-called data-sharing agreement. On the other hand, it may be appropriate to have some kind of agreement even during coordinated processing.[75]

In any case, the entity transmitting the data should normally ensure that the personal information is not processed in a manner that conflicts with the EU General Data Protection Regulation by the receiving party. The receiving party should, in turn, always ensure that the data subject has received accurate information about the transmission and that the collection of data was otherwise legal. In the long term, this may mean that coordinated management is needed with regards to a data subject exercising his or her rights, disclosure of information, regulating security measures and so on. Therefore, the difference

[75] cf. Kahn Pedersen, http://kahnpedersen.se/wp-content/uploads/2017/12/Johan_Kahn-Fredrik_Gustafsson.pdf;

compared to a mutual arrangement according to Article 26 of the EU General Data Protection Regulation does not appear to be especially great. From the standpoint of data security, the general conditions can contain an agreement that regulates the transmission of data from one controller to another (the Swedish Public Employment Service to employers/recruitment agencies). The things that should be regulated in the general conditions are: the purposes for which personal data may be processed, who is responsible for informing data subjects about what etc.

5.4.7 Legal basis for processing that occurs in the service

Apart from the General Data Protection Regulation and the act containing supplementary provisions to the EU General Data Protection Regulation (2018:218) (the data protection law), the processing of personal data carried out by the Swedish Public Employment Service is also regulated by the Swedish act regarding processing personal data in labour market policy activities (2002:546) - AF-PuL, and the ordinance on the processing of personal data in labour market policy activities (2002:623) - AF-PuF.

The Swedish Public Employment Service provides functionality in order to make it easier for individuals to look for work and for employers to find workers. It can be considered as being in the public interest (Article 6 (e) of the EU General Data Protection Regulation), that the Swedish Public Employment Service provide (as a service) an effective way for its customers to be able to come into contact with one another for the specific purpose of individuals being able to more effectively publish their applications for employment.

In the preparatory work for the data protection law[76] and in recital 45 of the EU General Data Protection Regulation, it is stated that the regulation does not require a specific law for each individual processing operation. Instead, it can suffice to have one law that serves as a basis for several processing operations, where such processing is necessary for performing a task carried out in the public interest. It is thus not required that each processing operation performed in the e-

[76] Government Bill 2017/18:105 p. 49.

service in question is established in national law. The processing of personal data that takes place in the user area can also be viewed as constituting part of activities on the labour market in view of the fact that the term "labour market activity" is very broad in application.[77] The purpose of processing the data must therefore find support in the authority's data registry law, AF-PuL. The purpose of compiling a CV that contains validated data for sharing with other parties applies to publishing applications for employment in accordance with Section 4, point 2 of the AF-PuL. Applications for employment are understood to be such documents or information that are usually included in an application for employment, such as contact details, a curriculum vitae and a personal letter. Section 3a of the AF-PuF specifies which personal information may be processed for this purpose; for example, driving licence information, education and previous employers. According to the second paragraph, personal data may be processed in order to publish applications for employment only if the job applicant has agreed to such processing. The consent referred to in Section 3a of the AF-PuF is a so-called privacy-enhancing measure and should not be viewed as a legal basis.

The job applicant is entitled to withdraw such given consent at any time, and if this is done, the personal data may no longer be processed for publishing applications for employment. According to Section 3a, consent can only be withdrawn when it applies to processing in the e-service (which is a processing operation that lasts for a very short length of time). Thereafter, the information has already arrived at the third party (employer/recruitment agency). A withdrawn consent can never cover the information already held by the third party. They have then taken over controllership. When consent has been

[77] In the preparatory work to AF-PuL, the government specified when the law could typically be applied. According to the government, the law might be applied when personal data relating to a job seeker, an employer or a point of contact are needed in order to perform the activities that the Swedish Public Employment Service is assigned to carry out.[1] However, this group of individuals can be increased on the condition that the processing of personal data takes place as part of the activities on the labour market.[2] According to the preparatory work for AF-PuL, the data registry law should not be applied when personal information is processed within the internal administration that lie beyond the direct core activity.[3] For example, outside the area of application are questions regarding staff, details about who is handling a certain matter or assignment, and what specialised expertise an administrator possesses.

withdrawn and come to the attention of the authority, any additional personal data about that individual may not be processed. However, the processing of information that has already been collected may continue. The service must have features that can maintain this. Personal data processed in the user area are not collected from the labour market database according to Section 7 of the AF-PuL, since the personal data are not used jointly in the organisation for the purposes stated in Sections 4-6 of the same law. The Swedish Public Employment Service must apply the EU General Data Protection Regulation when processing personal information outside of the labour market database. Additionally, the Swedish Public Employment Service must apply the supplementary provisions in Sections 1-6 of the AF-PuL and the supplementary data protection law.

5.4.8 Alternative legal basis specifically for processing in the form of personal retrieval and sharing

The Swedish Public Employment Service can be considered to have sufficient support for the processing operation of storage in the new functionality. It is conceivable that public interest will not be considered to cover the actual transmission of personal data to and from the user area. Consent in accordance with Article 6.1 (a) in the EU General Data Protection Regulation could constitute an alternative legal basis for processing personal data in the form of personal retrieval and personally sharing using the service; that is, only the actual transmission of personal data to and from the user area. It must be emphasised that consent as a legal basis may not under any circumstances replace or overlap a more appropriate legal basis that we deem to be in the public interest as shown above.

The scope for the authorities to base their processing operations on consent from the data subject is very limited. However, with regards to the type and nature of the e-service and the processing operation, the likelihood of an individual having actually willingly given consent to the processing operation appears to be high. Individuals have a genuine and free choice to use the new functionality, since the use of the service is *completely optional*. Individuals can without consequence refrain from using the functionality or withdraw their consent. It should therefore not be considered unlikely in any case that consent can be given on a voluntary

basis such as stipulated in recital 42 of the EU Data Protection Regulation.[78] Although it is possible that the processing involved in personal retrieval and sharing could be done on the legal basis of granted consent, this does not mean that the responsibility of the data controller ends; consent then constitutes the legal basis for processing personal data and is valid according the conditions set out in in the General Data Protection Regulation.

If consent is used, it is important to document the fact that it has been given and ensure that it is stored in an appropriate location (in a similar way to how information is kept in the user area). Logs may be retrieved and saved within the authority's information assets for ensuring removal or deletion according to the relevant decision. It is important to remember that documentation of consent is done for the sake of the authority and thus becomes an official document when received by the authority.

5.4.9 Personal retrieval of data for the user area

The fact that the Swedish Public Employment Service is the data controller for the content of the user area limits the way in which the area may be used and how information can be shared with third parties. It is the Swedish Public Employment Service that determines the conditions for how information may be processed so as to comply with applicable data protection rules.

Anna is able to use the new functionality to retrieve data that is *needed for her job search* as a preschool teacher. Anna does not have to personally enter the information and search for/retrieve documentation that supports her information. It is also validated since it was retrieved directly from the source.

The technical design for personal retrieval occurs in two stages. First, data is transmitted from the relevant authority's enterprise system to the user area

[78] Individuals are in no way obligated to give their consent, and they will not lose any positive effects if consent is not given; in fact, they even avoid some negative consequences by doing so. Consent must be given separately for the different purposes of personal retrieval and personal sharing. Consent is informed, since information is provided about the fact that the Swedish Public Employment Service is the data controller, about the purposes for processing, what information will be registered and processed, and the person's entitlement to withdraw their consent.

(Anna's) provided by that authority.[79] The new functionality thereafter provides integration for retrieval from the user area at that authority to Anna's user areas at the Swedish Public Employment Service. The feature is designed so that information can be retrieved only after Anna has made an *express request* and so that only the information that is needed for *that purpose is retrieved* without involving anyone other than *Anna, who submitted the request.* It does not make any difference that the data retrieved and shared is only a copy and is only shown in the e-service provided by the Swedish Public Employment Service. Presenting information is also a processing operation that the Swedish Public Employment Service is responsible for (according to the once only principle). It may be advantageous for the information only to be shown, since it reduces the number of stored copies (data minimisation).

On the other hand, the functionality could be limited so that the individual may not be able to process the information as desired. In accordance with Chapter 2, Section 31, second point of the Swedish Education Act (2010:800), Anna must present extracts from the original criminal records before she can be offered employment. Information involving offences does not constitute sensitive personal data for the purpose of the General Data Protection Regulation, but these data warrant special protection according to Article 10. The obligation to show an extract from the register applies regardless of whether the activities are run by a public or private organisation. In addition to the Swedish Education Act, the requirement for a background investigation is also defined by the act on record inspections for individuals who will work with children (*lagen (2013: 852) om registerkontroll av personer som ska arbeta med barn*). Provisions can also be found in the Criminal Records Act (*lagen (1998:620) om belastningsregister*). Within the scope of the new functionality, the Swedish Public Employment Service may not provide a feature to retrieve and share any information about Anna from the criminal records, since there is no legal basis for this processing operation. However, the extract from the register must be submitted to the one in the employing

[79] See also Section 2.1 of Annex 2

organisation who will decide whether to employ or accept Anna as a preschool teacher. However, Anna must not send this information via the new functionality; she should send it directly to the employer when it becomes relevant (and not through the Swedish Public Employment Service).

5.4.10 Transmission/personally sharing with a third party

Information can only be shared with a third party if the purpose falls within the scope of the authority's commission and only with clear consent from Anna. Data must thus always be transmitted as an active process in which the Swedish Public Employment Service provides the necessities for the process in question. Information from the user area may only be shared with other parties when it can be ensured that it will be done with a view to data protection.

Transmission of data from the user area cannot be considered to result in consequences for the authority on the basis of the way that the Freedom of the Press Act regulates official documents. Neither are any confidentiality issues expected to arise, since the authority cannot be considered to have transmitted documents from individuals' user areas.

In the event that it would be considered to be a dispatch according to the Freedom of the Press Act when information is transmitted from the user area, instead of the information being subject to secrecy according to Chapter 40, Section 5 of the Public Access to Information and Secrecy Act, it becomes subject to secrecy according to Chapter 28, Sections 11-12(a) of the same act. Secrecy then applies for information about an individual's personal circumstances unless it is certain that the information can be disclosed without causing injury to the individual or any of that person's immediate family and that the information is used in aiding a job search. If the job seeker has given consent to being presented to an employer, it can be assumed that it is in the job seeker's interest that this is done quickly, securely and smoothly. Secrecy intended to protect an individual does not prevent information from being given to another person if the individual has personally given their consent (Chapter 10 Section 1, and Chapter 12 of the Public Access to Information and Secrecy Act). A feature must therefore be provided for giving

such consent, and it must be saved so that it can be clearly seen that consent has been given and what the job seeker has consented to.

Our assessment is that, since it is the individual who for his or her own purposes shares the information by means of an electronic transmission, the rules for transmitting personal data via a medium for automatic processing according to the AF-PuF do not apply. However, articles 5(f) and 32 of the General Data Protection Regulation are applicable in order for the transmission to take place in a secure manner in the new functionality. In the event that the rules are considered to apply, there is support for transmission in Section 11(a) of the AF-PuF. It is there stipulated that personal data that may be processed according to Section 3 points 1 and 6 of the AF-PuF may also be transmitted to employers via a medium for automatic processing. The recruitment agency can in that case be considered a representative for employers.

Note that the third party must never have direct access to the individual's information in the user area. If the information is to be shared, it must be clearly separated for access (in some form of outbox) from all other information that is not to be shared. The retrieval or sharing of information to third parties must always be "logically separated as part of the total security solution."

- Design user interface so that the user must accept the terms of use for the e-service before it can be used, such as by clicking a checkbox.
- Design the user interface to include a location for clear and easily accessible information about the processing of personal data done in the e-service by the Swedish Public Employment Service (privacy notice).

5.4.11 Terms of use

The terms of use constitute an integral part of the user agreement that the user of the e-service enters into. It is particularly important that the terms of agreement are formulated correctly and clearly in order to prevent misuse and allow for legal measures to be taken against abuse of the e-service.

The aim of the proof of concept is to show how the ability of an individual to have insight and control over their data kept in the public – and in the long-term, also the private – sector can provide clear added value for the individual. Privacy and

personal retrieval and sharing has been at the core of the PoC development, and thus have also been the legal conditions for processing and sharing personal data. The PoC shows how an individual can retrieve data from various authorities and organisations in order to be able to create a CV at the Swedish Public Employment Service with validated information/data from validated sources (driving licence, employer, degree and educational information etc.), which can then be used to facilitate a job search.

The PoC provided is not a finished system that is ready for deployment. The PoC that has been developed should be viewed as an exploratory test implementation. The implementation[80] is a CV service that is integrated with a limited number of authorities and entities.

[80] As part of this assignment, we have not produced a general model for security and privacy issues, such as how a general operator should process and define which third party services are reliable for sharing data with.

6 Common model amongst public authorities for insight and control

In this chapter, we describe how a so-called user-centric data ecosystem that provides individuals with a better overview and increased insight and control over data about them kept by the public sector can be designed. The data ecosystem is described by means of a common model amongst public authorities that shows a desired movement in which information sharing is based on the needs of the individual and where that person is an active party in the sharing that takes place. The aim is that information that is already kept by public entities should be able to be reused in other contexts.

The common model amongst public authorities is conceptual, which means that the necessary movement would necessitate the addition or alteration of several fundamental prerequisites. This means that legal, technical, semantic and organisational prerequisites for the model need to be further investigated.

6.1 A conceptual model for individual insight and control

The government commission includes developing one or more solutions that could be applied jointly amongst public authorities in Swedish public administration in order to use digital tools to give individuals increased insight and control over the data about them that is found in the public sector.

As a part of this work, we have therefore developed a conceptual model to describe how a so-called user-centric data ecosystem could be designed to provide individuals with increased insight and control. We have then used the model in the being on sick leave life event (section 6.2). By using the conceptual model for this life event, we illustrate how digital tools for providing insight and control could generate benefits for the individual.

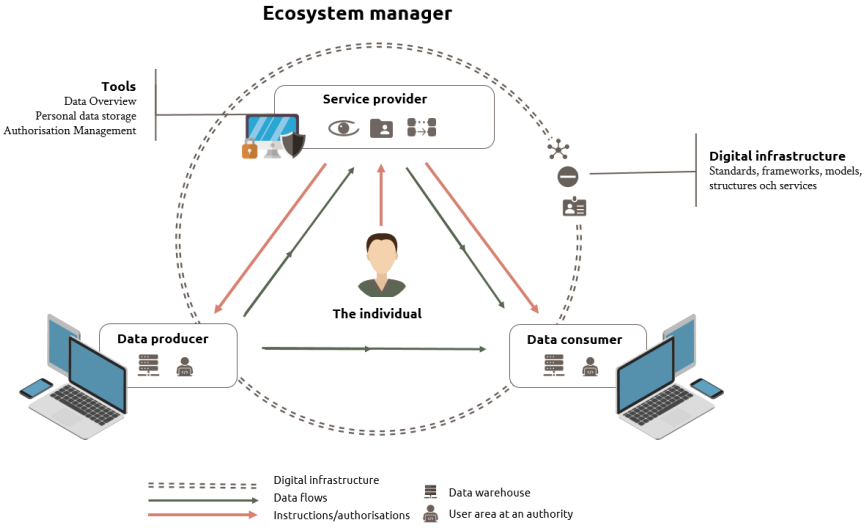
6.1.1 A user-centric data ecosystem

In order to find a common model for Swedish administration so as to facilitate insight and control for individuals into data kept about them by the public sector – and, in the long term, also information kept by the private sector – a conceptual model of a so-called user-centric data ecosystem is here presented. The model has been partially inspired by the concept of *user areas at authorities* as well as the

principles behind MyData and Solid, which are described in sections 6.1.3, 4.3.4 and 4.3.6.

The model is generic, which means that it describes the course of events in a general and universal way, but the model should also be able to be adapted and applied to specific situations and circumstances. Accordingly, the model can be implemented in different ways. For example, the model allows the individual to retrieve his or her data from a data producer to then share with a data consumer; it also allows data to be shared directly between a data producer and consumer without interim storage. The figure below shows the conceptual model of the user-centric data ecosystem.

Figure 5, The conceptual model of the user-centric data ecosystem



One idea with the user-centric data ecosystem is that it is the individual who uses various digital tools to determine when and how their data should be shared with other parties in the data ecosystem when the exchange of information between the entities is not regulated by law. The individual should be able to use the *Dataöversikt [Data Overview]* tool to see what information he or she is interested in accessing. The individual can then use the *Behörighetshantering [Authorisation Management]* tool to instruct (pink arrows) the data producer, which keeps the information in question in its data warehouse, to transmit the data.

The instruction also contains information on authorisation, which controls who, apart from the individual him or herself, should have access to the information.

6.1.2 The structure of the data ecosystem and its interested parties

The image of the data ecosystem shows a digital infrastructure that is controlled by an ecosystem manager, and there are also service providers, data producers and data consumers who have joined the data ecosystem, as well as private individuals. Different parties take on different roles depending on the situation.

- **The digital infrastructure** is illustrated with a blue double dashed circle that links together the various parties involved. The infrastructure consists of necessary functions and standards, as well as regulations that govern the application thereof.

- **The ecosystem manager** is the entity that provides and is responsible for the digital infrastructure with all the necessary functions for the user-centric data ecosystem. The digital infrastructure and its features can be provided by external suppliers (not illustrated). One example of an ecosystem manager is DIGG, which provides the infrastructure for Digital Post.

- **The service provider** is the entity that had joined the data ecosystem by accepting the technical and security requirements set by the ecosystem manager. A service provider makes available one or more digital tools that allow individuals to have insight and control over data kept by data producers and data consumers. Kivra is an example of a service provider that supplies a service to citizens based on the digital infrastructure for Digital Post that DIGG is responsible for providing.

- **The data producer** is an entity connected to the data ecosystem that processes personal information. The activities of the data producer may be public or private in nature; it may, for example, be an authority or a district health care centre. The data producer generates personal data that is stored in a data warehouse and used in the data producer's activities.

- **The data consumer** is the one receiving personal data from a data producer on behalf of the individual for whom the information applies, such as to handle a matter on the request of the individual. The information usually arrives at the data consumer's data warehouse. The data consumer is connected to the data ecosystem and may be a public or private entity, such as an authority or insurance agency.

- **The individual** is the identifiable natural person who uses digital tools to request insight into and control over data about them that is kept by the data producer or other parties in the data ecosystem.

6.1.3 Tools in the data ecosystem

In order to allow for an individual to be able to have insight and control over their personal data, a number of tools are needed. Tools refer to digital features that allow and facilitate an individual's insight and control. The model contains the Authorisation Management, Data Overview and Personal Data Warehouse tools made available by service providers. Aspects of these tools can be likened to functions of a digital wallet. Service providers can offer tools separately or integrated into one and the same digital service, such as a mobile application.

Data overview is a tool that provides an individual with insight into one or more data producers and a visual overview of data about the individual. The overview might, for example, show what information is stored, the legal basis for the processing operation, and the purpose for processing the information. The data overview can also contain information about how long the information will be stored and processed.

A personal data warehouse is a digital storage area where only the individual has insight and control over the information that is stored. Depending on how the information is processed, a personal data warehouse can in individual cases be a personal tool that allows information to be kept in interim storage until it is shared with the intended data consumer.

User area at an authority is a concept that means that an authority provides a protected area where individuals can process information and documents from the

authority without the authority or anyone else having access to the area. Information and documents in the user area should therefore not be considered official documents. A user area essentially corresponds to the personal data warehouse tool, the difference being that the user area can only be provided by authorities.

Authorisation management is the tool that allows an individual to be able to control and stipulate conditions authorising others to access their personal information, such as who is permitted to view, process and store the data, how long it may be stored for, and for what purpose it may be processed.

6.1.4 Digital infrastructure for the data ecosystem

The digital infrastructure consists of necessary functions and standards, as well as regulations that govern the application thereof. The infrastructure for the user-centric data ecosystem should as far as possible consist of the various building blocks that emerge within the scope of the common infrastructure for public authorities led by DIGG.

The building blocks that are developed within, for example, the Trust and security category should be able to form the basis of meeting the need for security within the data ecosystem. Within the Digital services category, the My Representatives, My Cases and My Profile building blocks could each or taken together make it possible for the data overview that is needed in the ecosystem. Standardisation for these three building blocks needs to be done and can serve as a guide for conceptual models and legal frameworks regarding how the information should be made available. One prerequisite for the entire model is that there are technical rules and frameworks governing how the extensive exchange of information should take place. The API management and Indexing building blocks may be important prerequisites for information exchange within the ecosystem.

6.1.5 Individual insight according to the model

In the user-centric data ecosystem, individuals are able to gain an overall picture of the type of data (about themselves) that is stored by various data producers. The *Data overview* tool can be used by the individual to ask whether any data about him or her is kept by any of the data producers or other entities connected to the data ecosystem.

Data producers and others that have joined the data ecosystem can respond to such a request from an individual in accordance with the stipulations that apply for being part of the data ecosystem. The *Data overview* tool could be based on so-called indexing, which involves scanning large quantities of data from different data producers in order to search for metadata about a certain individual. The metadata that is found from such a scan contains information that is sufficient for describing for the individual which data producer(s) hold data, the purposes for which data have been collected, the legal basis upon which data is processed by each data producer, and for how long data will be stored or processed.

The *Data overview* tool thus gives an individual insight into their data that is held by various data producers in a user-centric data ecosystem. According to the conceptual model, data producers can consist of entities from both the public and private sectors; that is, they can be authorities as well as businesses and other organisations.

6.1.6 Individual control according to the model

The user-centric data ecosystem is also intended to allow individuals to have control over such data stored by different data producers by means of various tools. The *Authorisation management* tool is intended to allow individuals to control and set conditions for others who will have access to information about them. The tool can, for example, be used to request or ask for corrections or deletions to be made to data, and for allowing data from a producer to be shared with a data consumer, or to cancel such an arrangement. The tool can also allow an individual to select the source from which certain information should be retrieved.

Data producers that are part of the data ecosystem must comply with the requests of individuals in line with what is specified in the conditions for joining the data ecosystem. Data producers must also comply with individual requests in relation to what is permitted by the data protection and public access to information and secrecy legislation.

In addition to sharing data directly from a data producer to a data consumer, individuals can also share information from the data producer with the data consumer via the *personal data warehouse* tool. The flow can be adapted as needed; that is, in accordance with what the situations and circumstances demand according to the regulations about information security, public access and secrecy, and data protection.

If an authority offers a digital service for sharing data etc., the authority may provide the service by means of the user area concept at an authority instead of using the personal data warehouse tool.

6.2 How the model can make a life event more straightforward

The following is based on the being on sick leave life event and uses the conceptual model to illustrate the added value that can be created for an individual when he or she is given insight and control over their data. The goal is to simplify an individual's interactions with public and private entities and to make it easier to submit correct information to them.

We assume that a person, who we call Anna, is sick for an extended period of time. This life event means that she needs to access and forward information that various different entities have about her. We have divided *being on sick leave* into three steps:

1. She seeks healthcare and receives a doctor's certificate.
2. She applies for sickness benefit from the Swedish Social Insurance Agency.
3. She applies for compensation from a private health insurance policy.

We shall now analyse Anna's need to contact and convey information to and between these entities. Then, in section 6.2.2, we shall present a hypothetical future scenario. In that scenario, we visualise how Anna is given insight and control over relevant data that she needs and that would simplify her interactions with the various entities.

6.2.1 Current situation

Anna seeks healthcare and the doctor determines that Anna is not able to work due to the symptoms of her illness. The doctor issues a doctor's certificate and asks Anna if she would like the certificate to be sent electronically directly to the Swedish Social Insurance Agency.

Since Anna also needs the certificate for her private health insurance policy, she asks to also receive a printout. According to Section 3 of the Patient Act (2014:821), the one responsible for keeping the patient records must issue certificates regarding healthcare upon the request of the patient. The doctor also asks Anna whether she consents to unified medical records, which allows the doctor to see what other doctors have entered in the records in connection with her previous visits to the doctor. Provisions regarding unified medical records can

be found in Chapter 6 of the Patient Data Act (2008:355). The district health care centre should in this case be considered a data producer, and the Swedish Social Insurance Agency as a data consumer.

Anna receives a text message from the Swedish Social Insurance Agency informing her that the agency has received a doctor's certificate, and she is asked whether she would like to apply for sickness benefit. Anna logs in to the e-services provided by the Swedish Social Insurance Agency and fills in the application. In order to complete the application, the Swedish Social Insurance Agency needs certain information about her employment and income that she needs to check up on. Before the Swedish Social Insurance Agency can make payments to her bank account, Anna also needs to update her contact and bank details.

Three months later, when Anna applies for compensation from her private health insurance policy, she needs to send the doctor's certificate and a copy of the decision granting sickness benefit.

In summary, the current situation provides Anna with limited possibilities to use digital tools to control what information is to be sent between the healthcare provider, the Swedish Social Insurance Agency and her private health insurance agency.

The life event also puts high demands on Anna, since she needs to act as both project manager and information carrier for sharing relevant data about herself between different parties, and the process is slow and administratively time consuming. She has a certain amount of insight, but no overview.

6.2.2 Hypothetical future scenario

This section aims to show a hypothetical future scenario in which things are made easier for the individual to provide information whilst simultaneously increasing insight and control over the individual's data. In order for this hypothetical future vision to become reality, several fundamental prerequisites need to come about or be changed.

In the following, we visualise the same life event in a hypothetical future scenario. We use the conceptual model to illustrate how Anna is given insight and control. The tools that are intended to give Anna insight and control are made available by service providers as described in section 5.1.2. The tools included in the conceptual model consist of three main components (*authorisation manager,*

personal data warehouse and data overview) that service providers can offer separately or integrated within one and the same service.

The goal is that:

- Anna is given insight and control by means of digital tools.
- Anna is helped to do things correctly.
- it is easier for Anna to provide information.
- resources are saved for Anna as well as society.

As a support in her interactions with both authorities and companies, and to manage her data, Anna makes use of various digital tools.

Using the *authorisation manager* tool, she has allowed authorities and public organisations to retrieve her contact information and, where relevant, her bank details. Accordingly, Anna only needs to keep her information up to date in the service made available by the service provider. Authorities and other organisations can then always receive her current details. A long time ago, she also used the authorisation manager to agree to unified medical records between her district health care centre and the specialised clinics where she receives treatment for her chronic illness. Before her visit, the doctor has accessed her medical records from the specialised clinic in order to better understand the symptoms she described before the meeting and to make a better medical assessment. The district health care centre in this case is the data consumer and the specialised clinic is the data producer.

Figure 6, Data sharing in a hypothetical future scenario.

The doctor examines Anna and determines that she is not able to perform her work due to the illness and therefore issues a doctor's certificate. Anna would like the doctor to share the information in the doctor's certificate directly with the Swedish Social Insurance Agency. The doctor at the district health care centre is in this case the data producer and the Swedish Social Insurance Agency is the data consumer. Anna receives a notification in the digital service informing her that her doctor's certificate is now available in 1177's certificate service. In the timeline feature, she can see that the Swedish Social Insurance Agency has received the doctor's certificate, and Anna does not need to worry about whether it has been received or not. She also downloads the certificate to the personal data warehouse tool in the service.

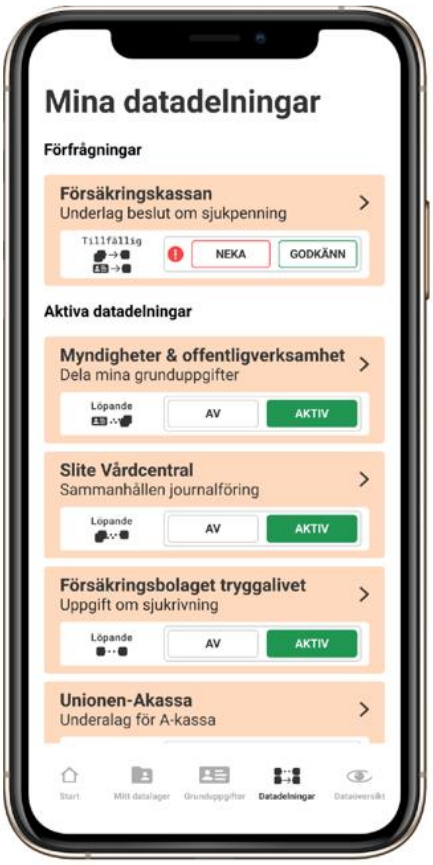
Anna receives a question from the Swedish Social Insurance Agency asking whether she intends to apply for sickness benefit. Since Anna would like to do so, she clicks on the link to My Account at the Swedish Social Insurance Agency to apply.

In order for the Swedish Social Insurance Agency to be able to make a decision about sickness benefit in her case, Anna needs to prove her income data and the percentage of full-time employment she works. Anna's employer has an electronic salary management system where information about the number of hours she works is stored. The employer also continuously reports payments and tax deductions digitally to the Swedish Tax Agency.

Anna can see in the *authorisation manager* for data sharing that the Swedish Social Insurance Agency would like to have access to these data. She can see in the tool that the purpose for collecting the information is "to make a decision regarding sickness benefit." Anna uses the tool to allow the Swedish Social Insurance Agency to retrieve the information right away. Her employer and the Swedish Tax Agency

in this case are data producers and the Swedish Social Insurance Agency is a data consumer.

Figure 7, Overview of data sharing in a hypothetical future scenario



Anna also has a private health insurance policy and has previously allowed her insurance agency to automatically receive information from the Swedish Social Insurance Agency when she has been off sick for three months. She receives a request from the insurance agency, which needs to access her doctor's certificate and decision regarding sickness benefit in order to handle the matter of her insurance. The Swedish Social Insurance Agency is now the data producer and her insurance agency is the data consumer.

For privacy reasons, Anna does not want outsiders to know that she is applying for compensation from her private insurance agency. She has therefore stipulated that the information first be downloaded to her personal data warehouse, which is a tool that only Anna herself has access to and where she can store information about herself. From there, she shares the doctor's certificate with the insurance agency.

Figure 8, Data sharing in a hypothetical future scenario

For Anna, it is a simple, quick and smooth process to share relevant information about herself that different entities are already in possession of. Providing data is also made much easier for her because the tools gradually lead her through the process and help her to do everything correctly. Anna can focus on her rehabilitation and eventual return to work.

The conceptual model and the hypothetical digital service and its tools should give Anna the needed overview of and insight into:

- what type of data is kept about her,
- which organisation is holdingdata about her,
- the purpose for which information is collected (processed).

in this future scenario, Anna also has control in that she can personally share and cancel the sharing of data about herself between different entities. Anna can also use the tool to download data in a structured and machine-readable format and forward it to another party without the entity that transmitted the data knowing what she intends to use them for.

7 Recommendations for continuing investigation

In working with this commission from the government, we have identified the fact that there is great value in giving private individuals increased insight and control over their data. It has also become apparent that there are several different ways of technically realising an arrangement that puts the individual in the centre, where they can be given an overview, insight and control.

Whilst we can see great potential in increasing user centricity with regards to the way data is processed, we can also see a need for other prerequisites to move at the same pace and direction. It has become clear that there is a potential conflict between an individual's entitlement to insight and control on the one hand, and the prerequisites for authorities to realise such insight and control on the other. We therefore highlight the following recommendations for further efforts relating to the issue of increased insight and control over personal data.

7.1 Needs assessments and analyses

It has not been possible within the scope of this government assignment to conduct investigations regarding the need of insight and control amongst the Swedish population and in what form it might take. For example, more knowledge is needed as to whether individuals want to have more sector-specific solutions for insight and control or whether they prefer complete solutions that span sector boundaries. When data spans large areas and has a high degree of detail, there is a risk of losing the possibility of gaining an overview that this commission aims to make possible.

We are therefore of the opinion that an investigation should be made regarding how users of tools and services for increased insight and control want these to be designed. The need of individuals must have a direct effect on how the tools, including data overview, should be designed and what functionality should be prioritised. The investigation should also result in an increased understanding of important design aspects for these tools. This can have a significant impact on the utilisation rate and is important for a design that is digitally inclusive.

7.2 Investigate the impact of specific building blocks on enabling increased insight and control for individuals

In the conceptual model presented in this report, we can see that some of the building blocks that are being developed or produced for the common digital infrastructure amongst public authorities could allow for user-centric ecosystems where the user has insight and control.

The building blocks fall mainly within the *digital services* category, which contains building blocks that allow for standardised digital services from public authorities for businesses and private individuals, and *trust* and *security*, which involve building blocks that allow for standardised digital functions for secure information exchange.

We propose that the possibility of increasing insight and control for individuals be further investigated within the scope of the My Representatives, My Cases and My Profile building blocks, which allow for the data overview that we feel is needed. Since the information in these building blocks is likely to be distributed at the source, we consider the Indexing building block an important prerequisite for allowing increased insight, since this mechanism points to the location of information about the relevant individual.

7.3 Investigate the possibility of promoting insight and control via authorities' user areas

The co-called user area at a public authority is already being used by agencies to provide services for private individuals and companies. When multi-agency solutions are employed for user areas and for sharing information to and from these areas, however, the legal situation is unclear. Our overall assessment is that, under the current system, it may be challenging for authorities to implement the individual interest of control in view of, amongst other things, the way that controllership is defined in the EU Data Protection Regulation, since it may potentially conflict with the ability that authorities have of providing services by means of the user area without details stored therein becoming official documents. The authority that provides a user area is the data controller for the processing operation that occurs in the area. Controllership implies many obligations in relation to the individuals whose personal information is processed. The authority must not have any real power over the information and documents that are processed in the user area in order for it to be considered as such according to the

regulations in the Freedom of the Press Act. It must therefore be clarified how these two conflicting interests can be united in sustainable solutions.

Information that is processed in the user area must also be necessary for the authority's operations. This means that, from the viewpoint of data protection, it is not possible for a user area at an authority to be used to process information in general without a connection to the activities of the authority. Such a limitation means that a user area at an authority can currently be used to provide an individual with increased control, but only within the field of activity that applies to that particular authority. It is therefore difficult to realise ideas about continuity, overview and control.

Since several relevant legal issues regarding user areas can currently be considered to be unsolved, we recommend that these be investigated further. An important part of this work is to examine the legal situation and the limitations regarding the scope of controllership in relation to the user area. Another important part is to investigate how the user area can be designed in such a way as to support user-centric data sharing within sectors or during life events. It would be beneficial for this work to be done in consultation with the Swedish Authority for Privacy Protection in order to bring about a proactive approach, and so as to more quickly highlight the need for adjusting regulations.

7.4 Develop the service obligations of authorities

Service obligations in accordance with Section 6 of the Administrative Procedure Act do not constitute a legal basis for processing personal data as brought up to date in the conceptual model or life events. Sharing information with other authorities and individuals, even when done on behalf of the individual in question, is thus not covered by the service obligations. The same applies for a possible exchange of information between authorities and private entities. Today, the way authorities process personal data is regulated by means of sector-specific legislation. The legal status for the digital transmission of information and the possibilities of providing individuals with insight and control can be considered uncertain.

If, on the other hand, the service obligations included disclosing and transmitting information to the individual and other authorities using digital media, authorities would have greater opportunities to provide for an individual's insight and control. As an example, such a service obligation could facilitate common

solutions amongst public authorities with regards to insight and control based on user areas and the transmission of digital information between authorities.

We suggest that an impact analysis should be conducted with regards to expanding the service obligations, along with one on the special data protection regulations (data registry laws) and the possibility of disclosing data in electronic form.