



**21SE03 - REFORMING THE SWEDISH PUBLIC EMPLOYMENT
SERVICE**
REFORM/IM2021/009

**Output 2: Addressing the legal and IT
challenges of data exchange to support
contracted-out employment services in
Sweden**

REPORT

January 2023



**Co-funded by
the European Union**

The project “Reforming the Swedish Public Employment Service” was co-funded by the European Union via the Technical Support Instrument (REFORM/IM2021/009). This publication was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

Table of contents

Abbreviations and Glossary	3
Executive Summary	4
1. Legal and IT aspects of data exchange and processing in Arbetsförmedlingen	7
1.1. Description of data exchanged and legal basis for use	8
1.2. Information technology capabilities in Arbetsförmedlingen	16
1.3. Use of data for research purposes	19
2. Information exchange in case study countries	21
2.1. Australia – <i>Workforce Australia</i> programme	21
2.2. Estonia – <i>X-road</i> data exchange technology	24
2.3. United Kingdom – <i>Restart</i> programme	27
3. Legal basis for information exchange in case study countries	30
3.1. Australia	30
3.2. Estonia	31
3.3. United Kingdom	32
4. Addressing information protection risks in case study countries	33
4.1. Australia	33
4.2. Estonia	35
4.3. United Kingdom	36
5. Lessons for Sweden based on experiences of other countries	37
References	46

Abbreviations and Glossary

AI - artificial intelligence

API - Application Programming Interface, a set of functions and procedures that enable automated data exchange (machine-to-machine communications) and allow for efficient cooperation between IT systems

Betyg – Swedish for “Rating”, it refers to the ratings system used to rate providers in Sweden with a statistical model, modelled after Australia’s Star Ratings

DESE – Department of Education, Skills and Employment; Australia’s authority administering employment services prior to July 2022

DEWR – Department of Employment and Workplace Relations, Australia’s authority administering employment services from July 2022

DWP – Department for Work and Pensions, the contracting authority for the United Kingdom’s employment services programmes.

EUIF – Estonian Unemployment Insurance Fund, the Estonian public employment service

GDPR – General Data Protection Regulation

ISKE – *InfoSüsteemide Kolmeastmeline Etalonturbe* (Estonian for “three-layered, front-line security of information systems”), an information security standard developed for the Estonian public sector.

ISO 70001 – an international standard on how to manage information security published by the International Organization for Standardization

KROM – *Kundval Rusta och Matcha*, a programme of contracted-out employment services in Sweden introduced in 2020

IT – information technology

Mina Sidor – Swedish for “My Pages”, Arbetsförmedlingen’s main digital portal for jobseekers, employers and private providers

PES – Public Employment Service

PRaP – Provider Referral and Payments, the data exchange system used for automated information exchange with outside providers by the United Kingdom’s Department for Work and Pensions

RFFR – Right Fit For Risk, an information security management system for employment services providers in Australia

STOM – *Kundval Stöd och Matchning*, a large-scale trial programme of contracted-out employment services in Sweden running from 2014-21

Executive Summary

Sweden is currently undertaking a reform, which began in 2019, to significantly modify the provision of its publicly-financed employment services. A key feature of the reform is the contracting-out of job brokerage and counselling services to independent providers. As part of the reform, the mandate of the Swedish public employment service (PES), Arbetsförmedlingen, is shifting towards monitoring of providers and working with different stakeholders in guiding and implementing labour market policies. The reform aims to provide a more client-centred approach to employment services, with jobseekers who are referred to outside providers given the freedom to choose their preferred provider. In parallel, Arbetsförmedlingen has undergone a significant restructuring, with an increased role of digital services and a smaller physical presence – one that may in fact now be increased to ensure sufficient local coverage.

One of the key aspects of the reform relates to the data processing and exchange that will form the informational backbone of the reformed system. The nature of the reform means that information which previously would have remained in-house with Arbetsförmedlingen will need to be exchanged with outside providers and that obtaining data from additional registries will be even more important. The exchange of information that previously would have been retained within Arbetsförmedlingen – such as that relating to jobseeker characteristics or counsellor-client meetings – will need to be exchanged and processed by multiple actors. In addition, contracting-out employment services based on an outcome-based payment model requires additional information that is not strictly necessary if such services are provided in-house, such as information on educational and employment outcomes.

Contracting-out employment services raises two important implementation challenges relating to data exchange. The first relates to the legal basis for sharing and using data from different sources and the second relates to the information technology (IT) infrastructure enabling such an exchange. The aim of this report is to support Arbetsförmedlingen in establishing a well-developed infrastructure that will support its new system and will facilitate the secure data exchange between private providers, Arbetsförmedlingen and researchers. Describing in detail good practices from Australia, Estonia, and the United Kingdom, it incorporates information gathered during interviews with multiple stakeholders in Sweden and the case study countries, countries' own public documentation and other OECD resources. The report has been drafted by OECD staff together with two sets of consultants with expertise in the areas of privacy law and IT.

The report draws on the reform proposals outlined in government documents and in the newly adopted legislation. Given that important aspects of the reform need to be implemented by Arbetsförmedlingen, it also uses as a reference point the ongoing *Kundval Rusta och Matcha* (KROM) programme of contracted-out employment services. First introduced as a trial programme in March 2020, this programme has been operating across Sweden since January 2022 and forms the basis for the reform.

The key assessments in this report are as follows:

- **A lack of data exchange in Sweden's current trial programme of contracted-out employment services imposes a considerable burden on jobseekers, private providers and Arbetsförmedlingen.** Arbetsförmedlingen's business processes currently rely heavily on information collected directly from clients, with relatively limited access to external public data sources. The current data management practises result in multiple parties collecting and managing similar data in their own silos, with providers collecting information on jobseekers that Arbetsförmedlingen already possesses. Having such parallel flows, storage, and management of data leads to duplicate data entities, which can lead to problems with data consistency, comparability, and reliability. Furthermore, the current reporting requirements are burdensome to providers. While reporting is of course necessary from a monitoring perspective, it is unclear to

what extent the information currently gathered is useful to Arbetsförmedlingen for this purpose. In its present form, the data collected also appear difficult to use for research purposes.

- **Rich administrative data combining multiple sources are available for research purposes in Sweden**, and it would make sense to have a similarly rich set of data available for operational use. The fact that rich and detailed individual-level data are combined from many different administrative sources and widely used for research purposes in Sweden underscores the lack of technical barriers to doing so. It also suggests that the presence of the strong legal and IT safeguards to maintain data confidentiality – such as are in place for using data for research purposes - can facilitate the wider use of such data.
- **The roadblocks to sharing data relate mainly to the legal basis and personal data security.** Arbetsförmedlingen’s overall IT system architecture is modern and up to date, and it is actively engaging with Sweden’s Agency for Digital Government, DIGG, to facilitate data exchange between various registries. Arbetsförmedlingen has also made significant investments in technology and modern agile ways of working to enable the development of its digital platforms. Legislative changes that took effect on 1 December 2022 have considerably expanded the scope of data that can be shared with private providers, but Arbetsförmedlingen still lacks a clear legal basis for accessing some relevant public databases and for passing on important information to private providers. Despite the recent enactment of legislation which has clarified the use of jobseekers’ data by outside providers – for example, explicitly granting them permission to process sensitive data – Arbetsförmedlingen’s current position of treating outside providers as legally being considered “data processors” (instead of “data controllers”) places severe limits on how providers can legally use jobseekers’ data.
- **A streamlined data exchange can enable novel features.** In addition to improving the efficiency of the system by lowering administrative burdens and increasing transparency, a streamlined data exchange could pave the way for novel features to be implemented in the reformed system. For example, with access to up-to-date income data, the outcome-based payments in payment model can incorporate a measure of jobseeker earnings to give employment services providers a financial incentive to place their clients into high-paying jobs. This approach has been adopted by the United Kingdom with its *Restart* programme, where payments to providers are progressively triggered after their clients reach certain earnings thresholds. A streamlined data exchange can also facilitate real-time monitoring and benchmarking of provider performance. In addition to facilitating monitoring, giving providers up-to-date information on their performance relative to their peers could help improve their service delivery and ensure a more consistent quality of services across providers.

Based on these assessments, the Swedish authorities should consider the following recommendations:

- **Arbetsförmedlingen could impose more stringent, risk-based data security requirements on private providers to improve security and address data security concerns.** While private providers are bound by the legislation governing data protection and the criminal liability provisions introduced in recent legislative changes, no specific data security requirements are in place to address data protection risks in Sweden. Given the potential risks associated with a data confidentiality breach and the uncertainty regarding private providers’ information security protocols, this arguably represents an important barrier to expanding the scale and scope of data sharing between various stakeholders. In the other OECD countries examined in greater detail in this report – Australia, Estonia, the United Kingdom – outside providers are generally required to abide by detailed information security management protocols to protect the sensitive information they hold. Given the presence of smaller providers in the Swedish system, Sweden could adopt a risk-based approach to the certification of providers like what has been adopted in Australia. Under such a system, larger providers could be required to meet the more stringent information security requirements, but in return, they could receive access to a wider array of information.

- **Arbetsförmedlingen could take additional steps to facilitate data exchange.** Giving private providers a stronger voice in developing Arbetsförmedlingen’s data exchange platforms could go a long way in facilitating information exchange. In Australia, the contracting authority has taken a role as an enabler for digital co-operation between providers and the public entities. Arbetsförmedlingen should consider looking into the Australian practises in creating a shared digital landscape for providing employment services with private providers. Furthermore, in the longer-term, Arbetsförmedlingen should have a goal of establishing data exchange standards that would enable data portability. This could entail a two-way seamless transfer of data between a provider and Arbetsförmedlingen, facilitating the monitoring functions of Arbetsförmedlingen while also strengthening the competitive market forces fostered by low costs of switching providers.
- **The Swedish government should consider adopting a “once-only” principle for essential data relating to employment services:** jobseekers should not have to provide such data multiple times. Overcoming legal hurdles for data sharing should recognise that data essential for the provision of employment services – such as information on prior employment and education – will be obtained from individuals even in the absence of any automated data sharing. However, the existing system results in an additional data reporting and collecting burden on all parties involved -- jobseekers, private providers and Arbetsförmedlingen. Sweden should consider adopting the “once-only” principle for essential data, a principle advocated by its Agency for Digital Government and fully implemented in Estonia: a citizen should need to provide a given piece of information to a government entity only once. To balance this principle with concerns relating to data privacy, more sensitive data could be subject to individual consent: for example, an individual could “opt-out” from having any information from a disability database shared with providers.

1. Legal and IT aspects of data exchange and processing in Arbetsförmedlingen

The Swedish Public Employment Service, Arbetsförmedlingen, is in the process of a major transformation. The reform will result in the contracting-out of a significant amount of employment services to independent providers in a quasi-market structure. Arbetsförmedlingen's mandate is to focus more towards monitoring of providers and working with different stakeholders in guiding and implementing labour market policy (Ministry of Employment, 2021^[1]). Preparations for the new system, in which matching of jobseekers and employers will be managed and operated by private providers or contractors, are ongoing (Arbetsförmedlingen, 2022^[2]). The reform will build on lessons learned from the implementation of the large-scale programme *Kundval Rusta och Matcha* (KROM) programme. Since 2014, *Arbetsförmedlingen* has been progressively engaging in larger-scale contracting of its employment services, including job brokerage and counselling services. The STOM programme was introduced in 2014 to contract out services especially for disadvantaged jobseekers (e.g. unemployed with low education levels, migrants, disabilities or aged 55-64 years) to independent providers. In March 2020, KROM was introduced as a trial programme in six of the existing delivery areas. Over the course of 2021, the programme was rolled out in the remainder of Sweden (Langenbucher and Vodopivec, 2022^[3]). The KROM programme remains in place today and forms the basis of the reform.

While important components of the reform still need to be implemented by Arbetsförmedlingen, the main elements have been set out by the government in numerous government documents as well as in newly adopted legislation (Ministry of Employment, 2021^[1]; The Swedish Government, 2022^[4]; The Swedish Government, 2022^[5]; Sveriges Riksdag, 2022^[6]; Sveriges Riksdag, 2022^[7]; Sveriges Riksdag, 2022^[8]). With regards to target groups, the new system is planned to provide contracted-out services for the broad “middle group” of jobseekers who are neither very close to nor very far away from the labour market. Providers are to be given financial incentives for sustained employment or education outcomes and clients are to be given the opportunity to influence the choice of provider as much as possible. Providers applying for contracts must meet several criteria including financial and organisational requirements. Arbetsförmedlingen will start the procurement of the new services in early 2023 in parallel with an update of the tender requirements of the current KROM programme (Carlsson, Román and Phalén, 2022^[9]).

Contracting out employment services in a manner such as is envisioned with the Swedish reform requires extensive data exchange between Arbetsförmedlingen and many external actors. This includes other public authorities (e.g. the tax authority), the contracted providers of employment services, and other third parties (e.g. researchers). Such data exchanges are necessary to carry out a variety of different tasks, including conducting administrative processes (e.g. client non-compliance procedures), monitoring providers (e.g. checking adherence to minimum service standards and comparing performance metrics), processing payment information (e.g. checking benefit eligibility) and conducting labour market research.

Arbetsförmedlingen's transformation plan for 2023-26 envisions that during 2023 the agency will continue to develop improved information exchange between jobseekers, the agency and providers of services (Carlsson, Román and Phalén, 2022^[9]). This is in line with instructions from the Swedish government (The Swedish Government, 2022^[5]). The Arbetsförmedlingen reform process includes an introduction of new digital solutions to make the employment service experience more streamlined for all the parties. As changes are happening in multiple levels, it is valuable to have a general assessment of Arbetsförmedlingen's IT-capabilities and understand the state of the relevant information flows around the contracted provision of employment services.

Ensuring an adequate legal basis for exchanging and processing information is another imperative. All of these processes need to be reconciled with the EU General Data Protection Regulation (EU) 2016/679 (GDPR) and the Swedish national legislation on privacy and personal data protection. Arbetsförmedlingen has already proposed changes to the Swedish national legislation to be able to access more data from other government agencies.

This chapter provides a description on the current state of Arbetsförmedlingen's IT-capabilities, data management and legal basis for information exchange relevant for contracted-out employment services. The information is based on interviews with Arbetsförmedlingen, Swedish employment service providers, and other stakeholders within Sweden. It is also based on desk research reviewing literature and other documentation. It was conducted by OECD staff together with consultants with expertise in the areas of privacy law and IT.

1.1. Description of data exchanged and legal basis for use

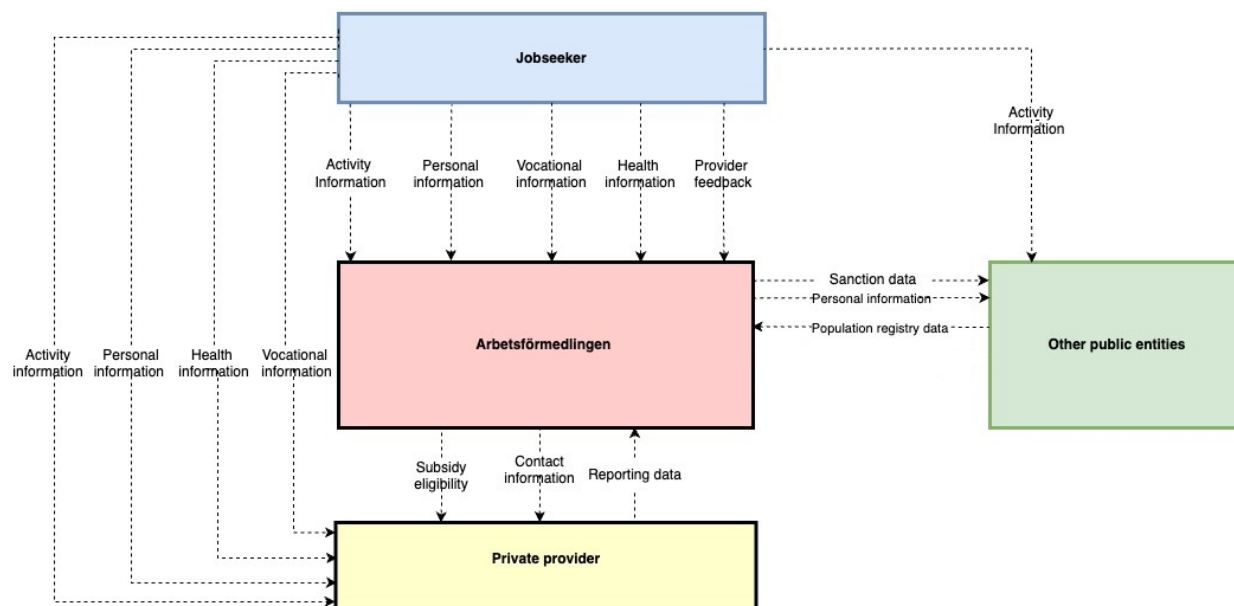
This section describes the existing state of data exchange in Arbetsförmedlingen relevant for contracted-out employment services, as well as the legal basis for it to be used by the various parties involved. It draws heavily on the existing state in the ongoing KROM programme, but also notes where changes are foreseen.

Data exchange between registers is limited

Arbetsförmedlingen collects an elaborate set of data on jobseekers, mostly directly from jobseekers as data exchange with other registers is very limited (Figure 1.1). In addition to personal information (e.g. contact details), Arbetsförmedlingen collects for example information on education, qualification and health limitations. These data are inserted manually either by the jobseeker (via a web-based user interface) or an employment counsellor (via an internal user interface). This is an inefficient process compared to automatic data exchanges with other registers, and also can result in lower data quality and accuracy.

Figure 1.1. Jobseekers currently provide the same information separately to Arbetsförmedlingen and private employment services providers in KROM

State of Arbetsförmedlingen information flows relevant to contracted-out employment services, September 2022



Note: The figure describes the state of information exchange implemented as of September 2022. As of 1 December 2022, the legal basis for additional information exchange was established, which included obtaining data from the tax authorities and sharing clients' individual action plans with private providers. The expanded legal basis does not include certain categories of information that could potentially be relevant, such as information on education outcomes or residency and permit information.

While much of the data relevant for employment services for providing services to jobseekers are collected directly from the jobseekers themselves, some data are also exchanged between Arbetsförmedlingen and other administrative registers in the current set-up. For example, Arbetsförmedlingen receives some information on registration of residents from the Swedish Tax Agency Skatteverket. Arbetsförmedlingen shares its register data with unemployment insurance funds and migration offices. However, due to legal rather than technical reasons, some data existing in other administrative registers and needed for service delivery (e.g. employment and education data) are not received from those registers, but collected instead via jobseekers (Arbetsförmedlingen, 2022^[10]). For some information jobseekers need to provide the same data even at several points in the overall process, providing the same information to Arbetsförmedlingen as well as to private providers.

Arbetsförmedlingen shares some jobseeker information with private providers for employment services, such as contact details and an employability rating based on an employment profiling score. The employment profiling score is calculated by Arbetsförmedlingen based on the more detailed socio-economic data of jobseekers collected during the registration process. This score is important for providers, as the payments they receive for placing jobseekers are contingent on them, with providers receiving higher payments for clients assessed as being more difficult to place (Langenbucher and Vodopivec, 2022^[31]). The monthly activity reports that jobseekers are required to file with Arbetsförmedlingen are currently not shared with the private providers (although Arbetsförmedlingen plans to change this in the future following the 1 December legislative changes (Carlsson, Román and Phalén, 2022^[9]) – see discussion below)

Private providers in KROM collect additional data from jobseekers and store and manage these in their own operational IT systems (customer management systems). Arbetsförmedlingen and private

providers collect and store similar data on jobseekers. However, these data are currently not shared between these entities. Legal change introduced in

At present, private providers in KROM need to file several types of reports with Arbetsförmedlingen. As discussed below, the delivery of these reports, however, is not supported by the IT system. These entail the following:

- An individual development plan (*individuell utvecklingsplan*¹) for each new client, detailing the activities to be undertaken by the participant including target occupations/jobs and specific short-term activities (this is to be made available to Arbetsförmedlingen upon request);
- A joint planning report setting out the provider's support plan for each new participant;
- Monthly periodic reports for each client summarizing the activities carried out including, on a daily basis, time spent interacting with the client (specifying face-to-face and otherwise), the types of support provided, and the types of activities the client has been undertaking;
- Deviation reports are to be submitted to report back on participants' absence and unmet obligations;
- Informative reports are used to request additional support from the PES (e.g. referral to other programmes); and
- A final report describing "what worked and what has not worked" and proposed next steps for the jobseeker.

Arbetsförmedlingen has three main interfaces enabling data exchange with jobseekers, private providers and other registers. Most of the data exchange with jobseekers and private providers takes place via a web-based user interface (online portal) called *Mina Sidor* ("My Pages"). Some data exchange takes place via the two APIs (Application Programming Interface - interface between registers), while some information exchange takes additionally place externally from interfaces. While most private providers rely on *Mina Sidor*, some private providers have developed custom solutions to integrate to Arbetsförmedlingen's APIs. These integrations currently provide contractors with basic contact and personal information of their clients. *Mina Sidor* and Arbetsförmedlingen's APIs allow only one-way transfers of information – from Arbetsförmedlingen to the employment services providers – but do not support having providers share data with Arbetsförmedlingen.

The lack of modern machine to machine integrations has resulted in a situation where data transfers between Arbetsförmedlingen, jobseekers and private providers are highly manual processes. In the case of *Mina Sidor*, the functionality for uploading encrypted files has not yet been implemented in the online portal. In the absence of secure digital channels for sharing documents, providers thus provide evidence on employment and educational outcomes in physical form, via regular mail. The challenge relating to employment outcomes will be sidestepped when the automatic data exchange between Arbetsförmedlingen and the tax authorities is implemented (the legal basis for such an exchange was established on 1 December 2022).

Furthermore, the current implementation with a lack of data exchange leads to duplicate data entities. Arbetsförmedlingen and private providers need partly the same data, which they currently collect, manage and store separately. Duplicate entities can cause issues in data consistency, comparability, and reliability. Data exchanges to support providing and contracting out employment services better are technically feasible but have not yet been implemented. Given the recent legislative changes, some of these challenges will be addressed when the enhanced data exchange foreseen in the legislation is fully implemented by Arbetsförmedlingen.

¹This is distinct from the individual action plan (*individuell handlingsplan*) drawn up for every registered jobseeker by Arbetsförmedlingen staff.

Current legal basis for processing and exchanging data for employment services in Sweden

The main legal basis for data processing and exchange relevant to contracted-out employment services administered by Arbetsförmedlingen are laid out in several pieces of legislation in Sweden. The first, the Act (2002: 546) on the processing of personal data in labour market policy activities, governs the lawful purposes of data processing, governs access to personal data within Arbetsförmedlingen, and specifies to which other entities Arbetsförmedlingen may disclose personal data.² The second, Ordinance (2002:623) on the processing of personal data in labour market policy activities, provides supplementary regulations to the Act (2002: 546) and specifies in detail which specific data can be used, by whom, and for what purpose.³ This legislation also specifies which information Arbetsförmedlingen may share with outside providers. The Ordinance (2000:628) on labour market policy activities outlines key aspects of Arbetsförmedlingen's active labour market policies, including certain data exchange.⁴ Underlying all of these laws is the EU's General Data Protection Regulation (EU/2016/679) as well as the Swedish law that is to supplement GDPR, the Data Protection Act (2018:218). Several key concepts relevant to this legislation are outlined in Box 1.1.

Several key legislative changes relevant to information exchange in contracted-out employment services went into effect on 1 December 2022. These include:

- an amendment to Ordinance (2000:628) on labour market policy activities which explicitly gives Arbetsförmedlingen the authority to issue regulations about which information private providers are obligated to supply to Arbetsförmedlingen (The Swedish Government, 2022_[11]),
- an amendment to Ordinance (2000:628) on labour market policy activities which provides the legal basis for private providers and their subcontractors to process sensitive personal data (The Swedish Government, 2022_[12]),
- changes allowing for extended access to and use of income data from the tax office for Arbetsförmedlingen,
- changes in the privacy act allowing the exchange of previously restricted information to be exchanged between Arbetsförmedlingen and private providers (The Swedish Government, 2022_[13]), and
- introducing the obligation of professional secrecy (*tystnadsplikt*) for suppliers (The Swedish Government, 2022_[13]).

² [Lag \(2002:546\)](#) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.

³ [Förordning \(2002:623\)](#) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.

⁴ [Förordning \(2000:628\)](#) om den arbetsmarknadspolitiska verksamheten.

Box 1.1. Key legal concepts from the EU General Data Protection Regulation (GDPR)

In effect since May 2018, the GDPR is the EU's overarching regulation on data protection and privacy. Its adoption was intended to introduce a more consistent set of data privacy rules across the EU.

The key concept used is the one of **personal data**, which is defined broadly to mean “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to... that natural person”. In the context of employment services, any data that can be directly or indirectly associated with an individual jobseeker is considered to be personal data and its processing subject to the GDPR.

GDPR adopts a broad definition for data **processing**, which is defined “as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

Certain categories **data that are particularly sensitive** merit especially strict limitations of processing according to GDPR and often require explicit consent to be processed (although public agencies such as Arbetsförmedlingen often rely on the concept of “substantial public interest” as a legal basis). These include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed solely to identify a human being, health-related data and data concerning a person's sex life or sexual orientation.

Another important legal distinction made in GDPR is between controllers and processors. **Controllers** can be considered the main decision-makers, as they exercise overall control over how, for what purpose and by which means personal data are processed. **Processors** execute the instructions of the relevant controller. If two controllers jointly determine for what purpose and by which means a set of personal data are processed, they are joint controllers.

In the context of contracted-out employment services, whether outside providers are considered controller or processors has important legal implications. It determines what providers are legally permitted to do with the information collected from jobseekers as well as their liability in case of a misuse of data.

In addition to being allowed to process specific categories of personal data, Arbetsförmedlingen is also specifically authorised to process certain categories of sensitive jobseeker data. It is authorised to process health and ethnicity data according to the Act (2002: 546), provided such data is necessary for the handling of a specific case. Rehabilitation information is further included in the system. On a similar case-by-case basis, Arbetsförmedlingen is further authorised to process personal data on offenses that include crimes, convictions in criminal cases, coercive measures in criminal proceedings, or administrative detentions. Such specific bases in the law are necessary considering the requirements of Articles 9 and 10 of the GDPR, which relate to the processing of such data.

Further information is included in the Individual Action Plan (*individuell handlingsplan*) for the jobseeker, which is currently not shared with providers but which Arbetsförmedlingen intends to begin sharing with providers in March 2023. This plan includes:

- the assessment of the jobseeker by Arbetsförmedlingen,
- the assessment of the jobseeker by the outside provider,

- planned activities and contributions,
- the jobseeker's obligations,
- the jobseeker's workwise and geographic focus.

Currently, any additional data collected by the outside providers directly from their clients is regulated only on a broad basis by GDPR. For example, outside providers could add special categories of data without Arbetsförmedlingen having clear insight in that regard. Arbetsförmedlingen contends that the private providers are to be considered data processors, while the private providers generally consider themselves to be data controllers. This legal distinction is important as it has implications for what providers are legally permitted to do with the information collected from jobseekers as well as their liability in case of a misuse of data.

Proposals for extending the scope of data exchange

Arbetsförmedlingen is currently limited in obtaining certain important information from other government entities because of the absence of a suitable legal basis. There is a statutory provision that enables access to the Swedish Tax Agency's database for the strict purposes of benefits calculation, while legislative changes from 1 December have also enabled broader use of this data. In addition, Arbetsförmedlingen uses jobseekers' bank identification credentials as means of signing-in and stores their social security numbers. Arbetsförmedlingen also receives information from other sources on an *ad hoc* basis, such as from the Swedish Prison and Probation Service, in order to provide services for incarcerated individuals and facilitate their reintegration into the labour market.

Consultations with Arbetsförmedlingen staff indicate that they would propose changing the current rules to expand the scope of personal data exchanged to facilitate its operations. This includes following-up on the activities of the outside providers, improving the *betyg* rating model for assessing and evaluating of outside providers, as well as enabling better labour market statistics. In order to enable access to relevant personal data, the proposals include data sharing obligations to be imposed on the Central Student Aid Board. According to the proposals, at the request of the Arbetsförmedlingen, the Central Student Aid Board would provide the following information about a jobseeker to the extent necessary for the labour market policy assessment, verification of the suppliers' right to compensation, and verification of the suppliers' results:

- social security number, coordination number,
- started training,
- interrupted training,
- completed training.

Arbetsförmedlingen also has plans to share more information about the jobseeker with the employment services providers (Carlsson, Román and Phalén, 2022^[9]). Changes to the Public Access to Information and Secrecy Act (2009:400) that went into force on 1 December 2022 expanded the legal basis for provider to access some new basic information about the jobseeker at the start of the service (The Swedish Government, 2022^[13]). In order to streamline the work in the reformed system, Arbetsförmedlingen intends to give outside providers access to their clients' individual action plans. This is to be implemented via the *Mina Sidor* platform. As a first step, from March 2023, providers will be given access to – but not allowed to directly modify – their clients' individual action plans. Future modifications to the platform are planned to give providers the ability to enter, for example, client activities and the focus of job search.

The Swedish government is engaging in efforts to create a common digital infrastructure for information sharing. Coordinated by Sweden's Agency for Digital Government, DIGG, it is bringing together multiple government agencies, including Arbetsförmedlingen, to develop common specifications,

standards, formats, working methods and requirements to support information exchange between the government agencies (The Swedish Government, 2022^[14]).

Automated processing of personal data for profiling jobseekers

The automated processing of personal data which has legal effects on jobseekers is subject to special data protection provisions in GDPR. In particular, the lawful basis for such processing has a more limited set of provisions than for other types of processing – notably, it does not include “task carried out in the public interest” as a possible legal basis. This has important implications for the implementation of the automated profiling of jobseekers, which assigns an employability score to a job seeker that is the basis for whether an individual is referred to contracted-out employment services.

Arbetsförmedlingen uses a profiling tool based on artificial intelligence (AI) to estimate jobseekers' distance to the labour market. It measures the likelihood of getting a job or other employment (fixed or indefinite term) within a six-month period. At the moment, up to 64 so-called data points are used for these purposes, including age, level of education, specialization in education, number of days registered at the Swedish Public Employment Service, postal code, country of birth and statistical data from Statistics Sweden concerning the postcode area. The scope of the data which can be used is outlined in Section 3 of the Ordinance (2002: 623). Based on that, a decision on the degree of support required by the jobseeker is determined (Arbetsförmedlingen, 2022^[15]). Whereas Arbetsförmedlingen has indicated that there is human intervention at the moment, the plan for the future is moving towards automated decision-making. There are two relevant legal questions concerning the personal data processing in this scenario: first, the processing of personal data required to train the model before it can be applied and second, its actual implementation to individual cases.

Currently, for processing individual cases, Arbetsförmedlingen relies on a rather cumbersome procedure based on jobseeker consent to establish a legal basis for conducting such processing. This is necessary because within the context of GDPR this type of jobseeker profiling qualifies, in the absence of human intervention, as automated individual decision-making which produces legal or similar effects.⁵ However, in addition to being cumbersome to implement in practice, this practice may not be consistent with guidelines on the use of consent issued by the European Data Protection Board (EDPB, 2020^[16]): “consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment” (p. 5). A sensible alternative would be for the national law to be amended to explicitly allow for profiling and automated decision making. This could also lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests – including, for example, a requirement that any decisions made based on profiling would need to be verified with meaningful input from Arbetsförmedlingen staff.

The legal basis for the model development and training is not subject to the same strict provisions as when it is used to determine whether specific individuals are referred to outside providers. Instead, it would be framed under the “planning, method development, supervision, follow-up, profit reporting and evaluation of activities” purpose contained in the third paragraph of § 4 of Section 3 of the Act (2002:546).

However, Arbetsförmedlingen arguably does not have lawful grounds for training the profiling model using sensitive data, such as health and ethnicity data. According to the Ordinance (2002:623)

⁵This is consistent with EDPB Guidelines 05/2020 on consent under Regulation 2016/679, whereby obtaining explicit consent in accordance with the conditions for valid consent in the GDPR would remain the only possible lawful exception to process this data. There is no contract between Arbetsförmedlingen and the jobseeker and there does not seem to be any law in Sweden which specifically regulates this scenario and lays down suitable measures in this context.

and the Act (2002:546), such data can only be processed for the handling of a case. As it could be difficult to argue that developing and training the statistical and AI model can be considered equivalent to the handling of a case, an amendment to the Ordinance (2002:623) and the Act (2002:546) may be required in order to provide explicit legal support to process this data for these purposes. Alternatively, a legal stipulation could establish that the development and training stages are seen as an inseparable part of the handling of a case.

A related question concerns the plans to enable the outside providers to use the profiling tool results to help the jobseeker. It could be argued that this falls under the Section 7.f of the Ordinance (2002:623) as part of the “information on instructions for applying for work and labour market policy programs” and “tasks that are part of an individual action plan”. Section 13.c of the same Ordinance would apply for the disclosure of the data on a medium for automated processing. Both the consent form used by Arbetsförmedlingen in this case and the Privacy Policy should thoroughly detail which data will be shared with outside providers and for what purposes, pointing out that outside providers will rely on the consent as their lawful basis to process this data.

Arbetsförmedlingen pointed out that it is not possible to completely anonymise the data when developing and applying statistical models. However, they believe that the data can be pseudonymised, which would be in line with Article 6.4 (e) GDPR. Regarding Arbetsförmedlingen’s ability to process data relating to the employment and educational outcomes – used, *inter alia*, to measure the success of performance of providers – it can be considered that this category would fall under “information needed as a basis for decisions on instructions for labour market policy programs or initiatives or for decisions on start-up jobs or state compensation for work in establishment jobs” of § 3 (10) of the Ordinance (2002:623) on the processing of personal data in labour market policy activities.

Automated processing of data relating to employment services providers

The statistical models used to monitor and assess outside providers and generate its *betyg* grades are not subject to the same strict limitations on data processing as those for jobseeker profiling. This is because it is used to help jobseekers make an informed choice of providers and to create incentives for the providers to deliver high quality services. Accordingly, Arbetsförmedlingen can rely on the public task lawful ground for processing, laid down by Ordinance (2007:1030). As such, this activity is within the permitted purposes for Arbetsförmedlingen to process personal data listed in § 4 of Section 3 of the Act (2002:546): “planning, method development, supervision, follow-up, profit reporting and evaluation of activities”.

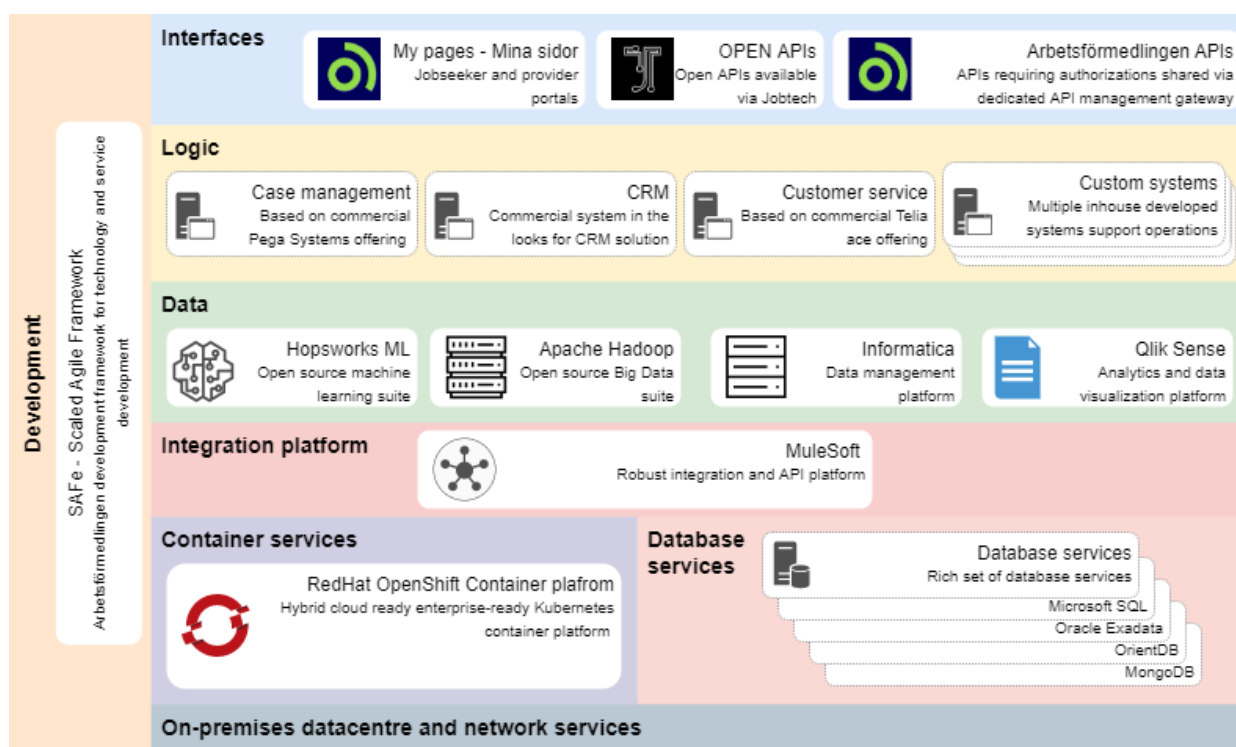
On the other hand, the legal basis for using certain external registry data sources to generate the *betyg* grades may need to be clarified. Obtaining data on employment and educational outcomes from administrative sources -- Central Student Aid Board and the Swedish Tax Agency -- would greatly facilitate the calculations of the *betyg* grades used to measure provider performance. For example, Arbetsförmedlingen could expand the outcomes measured to track jobseekers for several years and see the extent to which the providers efforts are having long-term effects on their clients. But the legal basis for using the data for this purpose may need to be explicitly established. Section 5 of the Act (2002: 546) allows Arbetsförmedlingen to process personal data for the provision of information needed within the Central Student Aid Board or the unemployment funds’ activities as a basis for decisions on and control of benefits, allowances and other support and the Swedish Tax Agency’s activities as a basis for decisions on and control of tax. Section 5.a of the same Act states that “personal data processed in accordance with Section 4 may also be processed for other purposes, provided that the data is not processed in a manner that is incompatible with the purpose for which the data was collected”. Whereas it is not clear whether this processing activity would fall under Section 4 as it is not explicitly defined in the Act, it arguably is compatible with the purpose for which the data was initially collected. It is an essential part of the process of connecting jobseekers with employers so it would meet the GDPR requirements on the link between

both purposes, the context in which the data has been collected, the nature of the data, and the possible consequences on the data subjects. Alternatively, the Act could be amended to expressly include this purpose.

1.2. Information technology capabilities in Arbetsförmedlingen

In recent years, Arbetsförmedlingen has invested heavily in its IT infrastructure and managed to modernise a significant part of it. All components of the IT infrastructure run inside Arbetsförmedlingen's own data centre facilities (physical buildings to house IT systems and associated components) due to current regulation and guidelines for Swedish governmental authorities. Figure 1.2 presents the aspects of Arbetsförmedlingen's technology stack relevant to contracted-out employment services (i.e., the parts relevant to the scope of this report and not the full IT infrastructure). The following sub-sections discuss the specific components of this part of the technology stack in detail.

Figure 1.2. Arbetsförmedlingen's technology stack overview



Note: Only the components relevant to the Arbetsförmedlingen's IT infrastructure components relevant to contracted-out employment services are described.

Some interfaces to support digital cooperation with private providers have been implemented

Arbetsförmedlingen has three main digital interfaces to interact with jobseekers, private providers and other stakeholders. One is direct user interface and two are API portals – the APIs are interfaces for machine-to-machine communications and allow efficient cooperation between systems. Currently, most data exchange takes place via the user interface.

The user interface Mina Sidor (My Pages) is the main digital portal for jobseekers, employers and private providers. Mina Sidor is a key part of the Arbetsförmedlingen's digital first mission and its objective is to make it easier for all the parties to cooperate (Arbetsförmedlingen, 2022[17]). Mina Sidor is currently still developing key features such as the ability to securely share information necessary for establishing employment outcomes of individual clients.

In terms of APIs, Arbetsförmedlingen has two interface options, Jobtech Development API portal and Arbetsförmedlingen's own API portal. The JobTech Development API portal provides an open digital ecosystem for collaboration and data sharing on digital job matching and guidance services (JobTech Development, 2022[18]). Open data initiatives like the JobTech API portal help Arbetsförmedlingen provide both data and a platform to share data for the general benefit of the labour market. Arbetsförmedlingen's own restricted API portal is used for specific and well-defined cooperation between Arbetsförmedlingen and its formal partners (Arbetsförmedlingen, 2022[19]). Arbetsförmedlingen's own restricted API portal is key capability to ensure effective digital cooperation with private providers.

The logic layer is being modernised

Arbetsförmedlingen's logic layer, which acts as an intermediary between the presentation layer and the data layer, has both commercial systems and internally purpose-built systems to support the core business functions. Commercial systems are purchased IT systems which have been adjusted to the needs of Arbetsförmedlingen. Utilising such systems allows Arbetsförmedlingen's internal development to focus on the capabilities that need to be flexible and cannot be easily acquired from the market.

Although legacy systems are still a problem in the logic layer, capabilities to address this are present and continuous modernisation of the systems is taking place. Arbetsförmedlingen has developed a roadmap to move towards a robust logic layer that would meet the objectives of Arbetsförmedlingen's business model, with an emphasis on the interconnectivity between the systems. Internal development of the systems and outsourced systems both aim at using modern tools and contemporary principles of IT architecture. For example, Arbetsförmedlingen is constantly renewing the custom systems stack using modern development principles like the microservice architecture. The microservice principles emphasise loosely coupled logic units (i.e. systems that are not tied down to a specific platform) to allow autonomous development and long-term agility. An effective use of microservice needs an holistic development framework and a flexible computing service, both of which Arbetsförmedlingen has (see more on this in the sub-section on computing services).

The technology to support data management and analytics is well set

A good set of data capabilities exists in Arbetsförmedlingen's technology stack, including capabilities to use machine learning. Using machine learning can increase the efficiency of operations via automation as it allows a system to learn from the data inside a process and make decisions based on the data. This should allow Arbetsförmedlingen to build processes that are less dependent on human interaction and free resources for other tasks. For data analytics, reports and visualisation, Arbetsförmedlingen uses Qlik Sense suite and for data management Informatica is being considered. Developments in using data better to support Arbetsförmedlingen's services are ongoing (e.g. for better tools of job recommendation or jobseeker profiling), while technology to support these new tools using data analytics is already well established.

Both open-source and commercial systems are in use in the data area. Given that open-source projects generally emphasize flexibility and aim to minimize any form of commitments, they give Arbetsförmedlingen the freedom to use these capabilities flexibly as needs arise. For example, the Hopsworks machine learning platform can be installed in all major cloud platforms on top of the option to

run it on-premises (Hopsworks, 2022^[20]). This kind of flexibility is important for Arbetsförmedlingen as many of the objectives of its digital-first strategy revolve around the effective use of data.

The integration platform allows Arbetsförmedlingen to integrate many systems

Arbetsförmedlingen has selected the MuleSoft platform as its main integration platform. The integration platform takes care of the connection between different systems and software. Arbetsförmedlingen has used many different systems to build its IT infrastructure and the integration platform is responsible for connecting these systems and allowing data exchange between them. MuleSoft is an industry leader in enterprise integrations (Pillai et al., 2021^[21]) and a reliable choice for providing this key capability. In addition to integrating the systems, Mulesoft enables Arbetsförmedlingen to develop APIs and manage the APIs.

Computing services support flexible application development

Arbetsförmedlingen has chosen the Open Shift container platform as the main technology for its computing services. A container is a unit of software that holds the necessary components for an application to run. The application code, runtime, system tools, system libraries, and software dependencies, among other components of an application can all be encapsulated to a container. A container platform enables a flexible application development by creating an abstraction layer between underlying infrastructure and the application. For developers this means more independence to build applications and thus faster lead times for implementation and deployments of new versions. For example, *Mina Sidor* gets its computing services from the Open Shift container platform.

Database services are sufficiently varied

Arbetsförmedlingen has a selection of database services available for different use cases. Databases are responsible for storing the data inside Arbetsförmedlingen's applications and systems. Applications have different needs for storing data and not all needs can be fulfilled with one database service. It is often necessary to implement a set of database service technologies to fulfil the needs of implemented applications. Arbetsförmedlingen has a very good variety of database services and this component should not be a limiting factor in the development of Arbetsförmedlingen's digital services.

On-premises data centres and networking services are a limitation to digitalisation

Arbetsförmedlingen hosts all the infrastructure in its own data centres. Public cloud platforms like Microsoft Azure and Amazon Web Service cannot be used due to the nature of the Arbetsförmedlingen's operations and the practices of the Swedish government. On the one hand, on-premises data centre services provide complete control over running digital systems and access to the premises, as well as complete control over network activity. For governmental authorities these are very valuable control layers. On the other hand, the management of a computing infrastructure requires significant investments and is resource intensive. Furthermore, the speed and scalability of private and public cloud offerings are not feasible in organisation's own on-premises installations. Individual actors cannot acquire computing capacity in similar ways as the exponentially larger public and private cloud computing service providers. For modern digital service development even well managed on-premises computing capacity will be a slowing factor.

Development practices rely on a modern framework

Arbetsförmedlingen uses the Scaled Agile Framework (SAFe) for managing the development of the information technology functions. SAFe is a framework to achieve a lean and agile enterprise focusing on principles such as alignment, collaboration, and delivery across many agile teams. SAFe scales these practices from the level of an individual developer to the level of the organisation or level at which a function is managed. Implementation of frameworks like SAFe usually lead to productivity benefits (Scaled Agile, 2021^[22]). To work well and efficiently, the SAFe framework needs the right tools and practices, and an adaptive organisational culture. Arbetsförmedlingen started to use the SAFe framework for its IT functions in early 2021. The tools required to facilitate this agile way of working exist and are in operation.

Arbetsförmedlingen's IT development practises are crucial to maximise the value-added of the infrastructure investments. Modern developments of digital services should be actively driven by the business needs and respond quickly to the changes in those needs. Arbetsförmedlingen has the infrastructure that can respond to its business needs well if development practises, business guidance and resources are sufficient. The adopted SAFe framework containing a set of well-defined principles for IT developments needs to be supported by an agile working culture, capable developers, effective and agile teams, as well as business guidance from teams across Arbetsförmedlingen.

1.3. Use of data for research purposes

Labour market research relevant to Arbetsförmedlingen's activities is generally conducted either through databases available internally at Arbetsförmedlingen or via a platform provided by Statistics Sweden, the national statistical agency.⁶ Data accessed through Arbetsförmedlingen have the benefit of being readily available with a minimal time lag but suffer from a lack of available data from other important registers. Conversely, the data accessed through Statistics Sweden allow for combining databases from various sources, but cannot be used for up-to-date monitoring or research that would incorporate very recent data. The rich databases available at Statistics Sweden have enabled rich body of academic research on topics relating to jobseeker transitions into employment, such as the role of employment counsellors, the effectiveness of specific labour market interventions or the stringency of activation requirements. However, the contracted provision of employment services raises new challenges relating to reporting of interactions between jobseekers and counsellors that threaten to hinder such research in Sweden in the future.

Statistics Sweden's individual-level database for research purposes, called *LISA*, enables researchers to access a rich set of data from administrative and survey sources (Statistics Sweden, 2022^[23]). Access to the individual-level data is through an online platform and enables researchers to access data on the entire population of working-age individuals in Sweden. The database includes a rich set of information on demographic characteristics, education and training, employment and unemployment, as well as income and social insurance (with the latter including information on health). The individual-level data can also be linked to family units and firms. The rich administrative datasets can also be enhanced by linking survey data, or information from other registers. However, the databases are made available with a considerable time lag – approximately 16 months for individual-level data. While such a lag is not typically problematic for academic research, it can present a challenge for other uses, such as monitoring programmes based on more sophisticated indicators than commonly-used ones (such as take-up rates, completion rates, etc). These include counterfactual impact evaluations examining a diverse set of outcomes such as employment and earnings.

⁶ In addition, IFAU, Sweden's Institute for Evaluation of Labour Market and Education policy, has access in-house to an individual-level database suitable for labour market research similar to what is available via Statistics Sweden.

Arbetsförmedlingen uses data available in-house for certain research and analytical purposes, such as the calculations of provider grades (*betyg* in Swedish). This means that the employment outcomes upon which the ratings are based rely on the outcomes reported (and monitored) by Arbetsförmedlingen, but they do not allow for including more sophisticated outcomes, such as those relating to earnings. Calculating such provider ratings from data held in-house is also necessary because it allows Arbetsförmedlingen to publish information on the performance of individual providers. By contrast, identifying individual providers would not be possible based on analyses conducted at Statistics Sweden, where the release of data to another public authority, such as Arbetsförmedlingen, would still be governed by data secrecy disallowing the identification of individual providers.

A parallel aspect to the above discussion of data access relates to the availability of data on the activities conducted by private providers. A large body of research has been conducted in Sweden examining various aspects of counselling and PES activities which requires detailed information on, for example, the attributes of counsellors or the frequency counsellor-client of meetings (Cederlöf, Söderström and Vikström, 2021^[24]; van den Berg and Vikström, 2014^[25]; Bennmarker, Skans and Vikman, 2013^[26]; Dahlberg et al., 2020^[27]). Research conducted by IFAU finds that reports filed by private providers in KROM for the purposes of fulfilling reporting requirements appear to be inconsistently filed by various providers, making their usefulness questionable. Analysing data from the reports supplied by the providers, Bennmarker et al. (2021^[28]) note that “we cannot determine in the data whether the supplier reported time separately for each activity, or reported the total time for the contact repeatedly. The data structure indicates that different suppliers have chosen different ways of reporting time” (p. 67). This means that the data are also not particularly useful for mapping the different service delivery approaches of the various providers – mapping the scope of individual development meetings and different types of individually adapted activities. Unless this challenge is resolved, the same limitations will apply and it will not, for example, be possible evaluate which elements of services provided are most effective and for whom.

An alternative approach to mandating detailed reporting requirements which can be used for research purposes is to periodically conducting similarly-detailed surveys amongst programme participants and link these to provider outcomes. Such an approach would recognise that the systematic and detailed reporting which is often necessary for research purposes is likely to impose a high administrative burden on providers. A survey-based evaluation approach has been successfully used in examining specific features of contracted-out employment programmes in Sweden in the past and has also been used in e.g. the Netherlands, the UK and Flanders (Belgium) (Langenbucher and Vodopivec, 2022^[3]).

2. Information exchange in case study countries

Examining how other OECD countries have addressed the legal and technical challenges relating to data exchange can help inform the design of similar aspects of the reformed Swedish system.

Despite considerable differences in the design of contracted out employment services through outcome-based payment schemes across OECD countries, they all face related challenges pertaining to the exchange of information between the contracting authority, the employment-services providers, other stakeholders and the clients. The case study countries described in this report each present interesting solutions to various aspects related to these challenges.

The report focuses on questions relating to the processing and exchanging of personal data with contracted employment service providers in three countries: Australia, Estonia, and the United Kingdom.

In Australia, external providers have been an integral part of publicly-funded employment services since 1998. After a recent reform of the employment services, it shares many similarities to the proposed Swedish system, including given jobseekers a choice of providers and referring the most employable jobseekers to online self-service tools. Estonia has been chosen as a comparison country due to its exceptional approach to data sharing and digitalisation between public administration actors and their clients. The Estonian model is based on the “once only” principle, where data is to be shared between the actors whenever it is required, and the data has already been once collected by a public institution. The United Kingdom has a purpose-built integration between two governmental agencies and is an interesting case on what is possible once such automated data exchanges have been established.

This and the next two chapters discusses the experiences of the three comparison countries relating to their data exchange for employment services.

This chapter provides some background on the case study countries and discusses which information relevant for employment services is exchanged in each of them. Chapter 3 discusses the legal basis for the information exchange in these countries, while Chapter 4 describes how they address information protection risks. The information presented was gathered from OECD resources, countries' own public documentation, as well as interviews with Australia's Department of Education, Skills and Employment (DESE),⁷ Australia's National Employment Services Association, the Estonian Unemployment Insurance Fund (Eesti Töötukassa) and the United Kingdom's Department for Work and Pensions (DWP).

2.1. Australia – Workforce Australia programme

Australia has a long tradition of contracted-out employment services. From its initial forays in the mid-1970s when it first started contracting to not-for-profit organisations, Australia underwent a significant transformation in 1998, when it replaced the *Commonwealth Employment Service* with contracted-out provision of employment services. Initially called the *Job Network*, the system has evolved over time, being

⁷ Following a restructuring after our meetings took place, since July 2022 the relevant institution overseeing contracted-out employment services in Australia is now the Department of Employment and Workplace Relations (DEWR).

replaced by *Jobs Services Australia* in 2009, which in turn was replaced by *jobactive* in July 2015, which ran through June 2022. Trials of a new model – the *New Employment Services Trial* (NEST) – started in 2019 introducing amongst other innovations the possibility for jobseekers to self-manage their unemployment spell through an online platform and a new payment model (Langenbucher and Vodopivec, 2022^[3]).

Workforce Australia, Australia’s current programme of contracted-out employment services

In July 2022, Australia introduced a new model of contracted out employment services called *Workforce Australia*. The transfer to the new contracting-out programme *Workforce Australia* represents a new and broader approach to online employment services. In the new programme, jobseekers sign up either online or through the Assisted Customer Claim call centre. Thereafter, jobseekers are profiled and segmented through a *Job Seeker Snapshot* (conducted either online or by phone), which includes several questions on the digital skills and access of the jobseekers. Based on the Job Seeker Snapshot as well as a phone interview, jobseekers are referred to appropriate employment service – either online services provided in-house by the department or in-person provided by contracted-out providers. The reformed system recently implemented in Australia thus shares many similar features of the proposed system to be enacted in Sweden, even though they each originated from different starting points.

The authority overseeing contracted-out employment services in Australia is the Department of Employment and Workplace Relations (DEWR). It was created in parallel to the introduction of *Workforce Australia* in July 2022. Up through June 2022, contracted-out employment services had been the responsibility of the Department of Education, Skills and Employment (DESE). This department was subsequently restructured into the Department of Education and DEWR (Department of Education, 2022^[29]).

Australia’s new approach represents a significant investment by the government in the development of self-service, online tools. *Workforce Australia Online* is a digital platform for jobseekers, employment service providers and employers built to enable a new digital first employment service for Australians. The service includes job search, job applications, career building services and the possibility to include a professional online profile. *Workforce Australia* also has obligatory reporting functions of those jobseekers that are not enrolled with a provider to ensure compliance with the income support programs (DESE, 2022^[30]). The platform provides services to businesses as well. An online platform, *Workforce Australia Online for Business*, allows employers to post job opportunities and search for workers. The online portal can act as a bridge between businesses and employment service providers. It can allow businesses to find workers from employ individuals from the more extensive provider driven programs and possibly get wage subsidies that are attached to the provider-led programs (DESE, 2022^[31]).

***Workforce Australia* was built on a modern IT-infrastructure with agile development practices.** Public cloud platforms provide flexibility and speed that traditional data centre services cannot easily provide. Modern IT infrastructure was a key enabler for the launch and development of *Workforce Australia*. The utilisation of agile DevOps-based development tools and practices⁸ was highlighted by DEWR itself as the most important technical capability enabling the development of the *Workforce Australia* platform. Efficient digital service development is possible only if the technical capabilities of the organisation are at a sufficient level. DEWR has extensively invested in a modern technology stack and has also fostered modern development tools and practices.

⁸ While there is no universal definition for DevOps, OECD (2019^[59]) describes it as follows: “DevOps is the combination of cultural philosophies, practices, and tools that increases an organisation’s ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organisations using traditional software development and infrastructure management processes” (p. 60).

The *Workforce Australia Online* platform is based on very similar technical capabilities to those used by Arbetsförmedlingen. The key difference between the two is that Australia made extensive use of public cloud technologies which is currently not possible for Arbetsförmedlingen. Nevertheless, Arbetsförmedlingen's investments in technical capabilities to reach similar level of DEWR technical capability are well justified and should continue.

The exchange of information in the Workforce Australia programme

Given the importance of information flows and data exchange in the reformed system, digital cooperation with all parties is critical for the success of the Australia's new approach. Given its relevance to the Swedish context, the focus of this report is on the interface between DEWR and the external service providers. Facilitating digital interactions taken by or with the jobseeker is an important goal for the new platform. *Workforce Australia* provides information on jobseeker's path to employment and gathers information from providers' activities to help that journey. This digital footprint allows DEWR to do performance monitoring both from the point of view of the jobseeker and from the point of view of the providers that help them.

Providers have several ways to interact with the *Workforce Australia* platform. The platform has an online user interface dedicated to the providers. This provider interface has export capabilities to enable the transfer of data to the providers own systems and features to report jointly agreed milestones. In addition to online interface, there are API capabilities. APIs will lead to largest time saving and performance benefits in the employment service digital transformation and are key target of DEWR. Exporting information is currently possible via APIs and providers appreciate the capabilities of the new platform, though the largest improvement will come from APIs that can input information to the DEWR systems. Those will eliminate manual inputs between the DEWR and provider systems. API development is led by DEWR. Providers do not have an active role in the API development but do state that they are technically capable to utilize any published interface.

At present, jobseekers may still need to input the same information multiple times, once with DEWR and again with the provider. This is partly due to work in progress status of the *Workforce Australia* platform. While API development is seen as the main solution for this problem – allowing providers to receive information on clients in automated manner –these capabilities will need to continue to exist in the web user interface as well (with the possibly to download client information in a machine-readable format). Providers can also access some common information about jobseekers placed with other providers, but data recorded by a given provider is only accessible to that provider and DEWR.

Despite having relatively advanced systems for transferring data between DEWR and individual employment services providers, DEWR at present has only limited automated information exchange with other government entities. DEWR has access to data from the income support system, but they do not have access to payroll data that would allow them to determine employment outcomes, wages or hours worked. Employment outcomes are reported by clients to the employment services providers, who then report these to DEWR. DEWR subsequently conducts follow-up surveys of (former) jobseekers to verify the reporting of providers.

Similarly, most of the information used to categorise individuals based on the profiling instrument relies on what is reported by the jobseeker. The personal data collected by the Job Seeker Snapshot questionnaire – and subsequently used to calculate the Jobseeker Classification Instrument score – comprises of 49 questions, not all of which are asked to all jobseekers (DSS, 2022^[32]; DEWR, 2022^[33]). These including special categories of data such as disability and medical conditions, which are optional for the jobseeker. A few of the data fields used in this profiling procedure are cross-checked with other sources, but most are not.

DEWR is keen to expand the usage of data sources from other government agencies to facilitate its contracted-out employment services operations. Tax records would be especially useful for performance monitoring of providers (similar to what is done in the United Kingdom – see Section 2.3) as well as for providing a more comprehensive assessment of jobseeker’s past employment history. Education records would eliminate some manual inputs from jobseekers.

One technical challenge experienced by Australia that has hindered the exchange of information from different sources is the lack of a universal identifier for individuals. Australia does not have such an identifier in place, meaning that systems-specific identifiers are used in e.g. the education databases and tax databases. In many cases, these also cannot be mapped from one system to another, meaning that it is often not technically feasible to automatically link data across databases (i.e., without clients providing the different identifiers themselves). A related challenge in linking the data from different administrative sources relates to the lack of a well-established legal basis for extensive intergovernmental digital data sharing (for a discussion of this aspect, see Section 3.1).

2.2. Estonia – X-road data exchange technology

Estonia is a world leader in terms of the digitalisation of government services (Azzopardi et al., 2020^[34]). Estonia’s path for digitalization began in the early 1990s, after Estonia’s independence following the collapse of the Soviet Union. Estonia had very limited legacy systems or resources, which presented an opportunity to build a technology infrastructure from scratch (E-Estonia Guide, 2022^[35]). Today, a wide array of government services are provided online and digital tools are widely used in government, including from the Estonian public employment service (the Estonian Unemployment Insurance Fund, EUIF).

Although the EUIF does rely on outside providers to provide employment services, the focus of the Estonian case study in this report is on the automated data exchange between its various government databases. The Estonian national level digital infrastructure is significantly different from the one in Sweden, and thus the example of the Estonian PES is not directly transferable to Arbetsförmedlingen. Nevertheless, the example does provide relevant insights and evidence on how a high level of integration can benefit all aspects of employment services. These insights and practises can be adapted to suit some of the Arbetsförmedlingen’s needs related to contracted-out employment services.

The Estonian government’s digitalisation efforts rest on several principles:

- **Decentralisation**, which means that no central databases exist, and public institutions and business alike can develop their digital systems independently.
- **Interoperability between system elements to ensure secure data exchange.** Integrity is guaranteed by using the KSI blockchain technology (a blockchain technology designed in Estonia) for data and information exchange. The KSI blockchain technology is an open platform, thus enabling any institutions to use the infrastructure as an open-source solution.
- **A no legacy policy**, supported by continuous investments in technology and amendments to regulation that adjusts the legal framework to accommodate the use of data while protecting data privacy.
- **A “once only” principle in data collection** whereby any data that needs to be provided to a government institution by an individual needs to be provided only once.⁹ Data are then shared

⁹ This principle does not apply to outside contractors providing government-funded services.

across public institutions (and exchanged securely with those needing these for their service provision, supported by legislation), preventing any duplicated data and minimising bureaucracy.¹⁰

- **Transparency** enables all citizens to see their personal information collected by administrative registers, as well as how these data are used by the public organisations (Ilves, 2021^[36]).
- **Unique national individual ID numbers** used by all public registers for identification of citizens (even though additional client numbers can also be used) to facilitate linking data across registers.

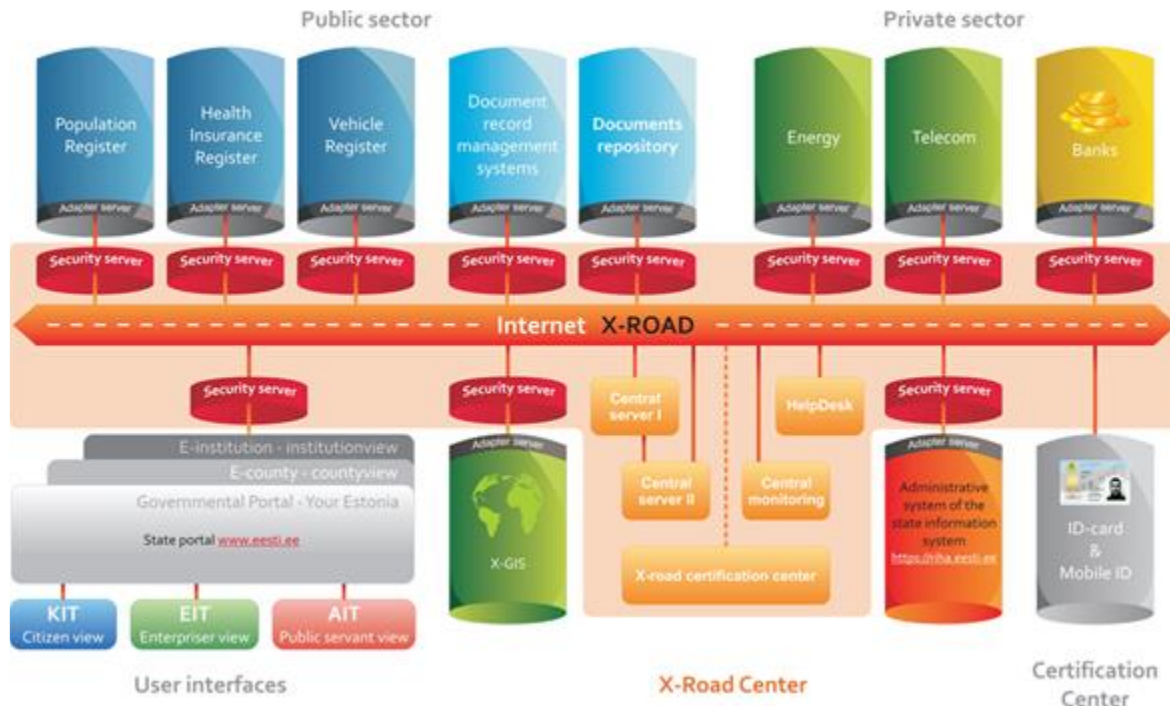
The X-road data exchange technology is the cornerstone of the Estonian national level digital infrastructure.¹¹ Comprising of a distributed information exchange platform, it enables interoperability and provides a low threshold for the stakeholders to access data in other registers (Figure 2.1). X-road has a versatile security solution, including authentication, multi-level authorisation, a high-level system for processing logs, and data traffic that is encrypted and signed (Republic of Estonia Information System Authority, 2022^[37]). This prevents data from being corrupted and inhibits access to data for unauthorised individuals or third parties. There are currently 3 100 data services set up using the X-road technology between 694 public and private institutions in Estonia.

¹⁰ Note that different implementations of such a principle may be possible. The United Kingdom, for example, has implemented a similar process for reporting a death to with its “Tell us Once” service, which allows an individual to report a death to most government organisations in one go (UK Government, 2022^[60]). The United Kingdom’s Tell Us Once program, although though data can be collected only once, each data record can appear in multiple database repositories across government entities (Rashid and Eaves, 2020^[61]).

¹¹ *X-Road* refers to the technology developed together by Estonia, Finland and Iceland through MTÜ Nordic Institute for Interoperability Solutions (Republic of Estonia Information System Authority, 2022^[62]). The data exchange layer used in Estonia is now called *X-tee*. Until 2018, it was named *X-Road* in English.

Figure 2.1. Estonia's X-road provides a platform for information exchange between numerous public and private entities

Estonian data and information flow diagram



Source: European Commission and Pieterston (2020^[38]).

The large amount of trusted data available and a high level of integration of digital systems have enabled the Estonian institutions to implement advanced technologies to support decision making and services. It is estimated that more than 50 AI-based tools are used in the Estonian public sector. For example, the EUIF has developed a tool called OTT to support its employment counsellors. The tool is designed to improve the understanding of jobseeker needs and estimate probabilities of different employment scenarios (entering employment, returning to unemployment). The tool also systematises jobseeker needs to better target support and re-allocate counsellor caseloads (Enterprise Estonia, 2021^[39]). The EUIF has adopted AI technologies also for its other business needs, such as matching jobseekers and vacancies.

X-road is the main data exchange technology used in the EUIF. Data are received from 30 different registers and used across the services and processes. The EUIF shares data using the X-road technology with many other institutions as well, such as with the Social Insurance Board, which uses the information as the basis for pension calculations (Mõttus, 2022^[40]). In addition to developing tools using AI technology to provide better services, the automatic data exchanges with other registers have enabled the EUIF to automatise many of its services and processes (e.g. processing benefit applications is fully automatic).

The use of X-road enables the EUIF to collect a large share of jobseeker data from different registers, rather than requiring them to collect them directly from jobseekers. If the jobseeker data exist in another register, the data are to be shared with the EUIF in case these are needed for the service provision (i.e. based on the tasks and data needs of the EUIF defined in legislation). For example, the EUIF can verify employment status using the data in the employment register, entrepreneurship status in the business register, and enrolment in the education system in the education register.

Currently, only one public-private integration has been implemented in the EUIF. Private organizations have to meet both legal requirements for data access and the information security standard ISKE to access *X-road*. The main reason for the small number of public-private integrations is the complexity and cost of meeting ISKE requirements (for a detailed discussion of this topic, see Section 3.2).

In addition to *X-road*, the EUIF has a user interface for external stakeholders (a self-service portal) and secure emails as digital channels for data exchange. The self-service portal enables jobseekers, employers and service providers to see information regarding their services, as well as insert information, for example jobseekers to apply for services, employers to post vacancies, service providers to share reports on participants, etc. Some information can also be uploaded in XML format, for example to post job vacancies. Encrypted emails are used in addition for irregular small enquiries, but caution is applied because additional human interaction increases the chances of errors that might result in data breaches.

2.3. United Kingdom – Restart programme

The United Kingdom has a long history of contracting-out employment services for jobseekers to independent providers for a range of different client groups. Since the first performance-based contracts were introduced in the late 1980s, the country has adopted a number of programmes contracting-out employment services and adopting different commissioning strategies (Langenbucher and Vodopivec, 2022^[3]). A notable shift in the United Kingdom’s commission strategy began in 2008, with the aim to overhaul the system of contracted-out employment services to develop more strategic relationships with providers. The central elements were the so-called “prime provider” model, with large and long contracts, mainly outcome-based funding with a focus on sustained outcomes, and minimal service prescription through a “black box” delivery model. Subsequent programmes, such as the *Work Programme*, followed this model, rewarding providers for placing clients into employment for up to two years after they initially became employed. Although the programmes can be judged to be successful according to several metrics, the lack of automated data exchange did result in considerable administrative burden of providing evidence for sustainment payments and issues with the validation process (Foster, S. et al., 2014^[41]).

To address the data exchange challenges inherent in contracted-out employment service, the United Kingdom employed automated data exchange when it introduced a new programme of contracted provision of employment services called *Restart* in the summer of 2021.¹² Launched in July 2021 across England and Wales, *Restart* will run for three years, targeting long-term unemployed (12 to 18 months unemployed) recipients of means-tested unemployment benefits (Universal Credit). In total, the contracting authority administering the scheme – the Department for Work and Pensions (DWP) – expects to refer one million jobseekers to *Restart* over the three-year period.

Automated data exchange on earnings - Provider Referral and Payments (PRaP)

The case study of the United Kingdom is based on the *Restart* programme and focuses on the automated data exchange system, *Provider Referral and Payments (PRaP)*, used in that scheme. The PRaP system links data from the tax agency participant tax information to verify employment outcomes (DWP, 2022^[42]). PRaP is not the only digital tool used in Department for Work and Pension to provide employment service. DWP providers have access to an online job search portal for jobseekers, and the same platform can be used by business to advertise vacancies (GOV.UK, 2022^[43]). Within *Restart*, other systems are used to facilitate the cooperation. For example, in *Restart* a system called *Jaggae* is used for in sharing deliverables, documents and reports from providers to the Department for Work and Pension (DWP, 2022^[42]). Systems like PRaP required that DWP established integration, data management and

¹² The automated data exchange was first introduced in 2017, when DWP rolled out the *Work and Health Programme*, a programme designed for individuals with disabilities and as well as the long-term unemployed.

reporting capabilities. The operational and IT-capabilities required are similar to what is present in the Arbetsförmedlingen technology stack.

The PRaP system is used in a few key ways to facilitate the goals of the *Restart* programme. The main use is for the automatic employment milestone reporting based on the participants' tax records. In contrast to previous programmes administered by DWP such as the *Work Programme*, providers do not need to provide any evidence of earnings or submit a claim for payment. PRaP is also used as part of both provider and jobseeker performance and compliance monitoring, as well as to give employment services providers detailed client information upon their referral from DWP (DWP, 2022^[42]).

Similar to most outcome-based contracted-out employment programmes in OECD countries, the payment scheme in *Restart* is heavily contingent on outcomes achieved (Langenbucher and Vodopivec, 2022^[3]). Provider compensation is based on delivery fee and job outcome payment. Attachment fees linked to client referrals equate to roughly 30% of the total contract value and job outcome payments account for the remaining share (DWP, 2022^[42]). With the integration between the DWP and United Kingdom's tax authority, data for employment are received in near real time.

The *Restart* programme has adopted a novel payment scheme that is made possible by the use of the automated data exchange. *Restart* has five milestones which "trigger" a notification to the provider and DWP: one when participant has started a job; one each when earnings thresholds of GBP 1 000, GBP 2 000 and roughly GBP 3 900 have been attained;¹³ and one if a participant's employment has ended. Providers do not get direct access to the tax information – PRaP generalizes the data to the milestones that provide just enough information required for monitoring the progress (DWP, 2022^[42]). The parameters of the payment model are made possible due to DWP access to participant's tax records. Without this integration follow up and confirmation of the outcomes could be too time consuming to monitor and to confirm. These thresholds are also a valuable tool to follow up the participant progress in the program with minimal work from all parties. Providers can use PRaP to monitor participants' progress and possibly proactively contact participants, such as when an individual's employment ends.

PRaP utilization is not limited to provider milestone follow up. Provider compliance is followed with assistance of PRaP. Provider audits are based random participant progress audit selection in the PRaP systems. These participant cases are reviewed by Department for Work and Pension performance compliance officers in detail in the providers' systems (DWP, 2022^[42]). PRaP information is also useful for a more general performance reviews of the scheme and its outcomes, enabling a factual comparison to other programmes and facilitating the overall success of the scheme.

Despite its considerable benefits, the PRaP system has some shortcomings. The main one relates to the inability to distinguish between several different types of reported income from participants. For example, the tax information on income does not distinguish whether a participant has been self-employed. Partly for this reason, earnings from self-employment also count towards the earnings thresholds that trigger outcome payments to *Restart* providers. In addition, DWP has difficulty distinguishing other types of income which do not count towards the earnings thresholds, such as tax refunds or payments made while individuals are receiving employment subsidies. In such cases, providers are required to notify DWP separately to clarify that such payments have been made (and, presumably, clients have a duty to report this to the providers).

Non-earnings related data exchange in the *Restart* programme

Apart from the data on client milestones attained, DWP gives employment services providers a rich set of information on the client upon referral. Information received by providers includes an individual's

¹³ The precise amount for the final earnings threshold is tied to the National Living Wage; it is calculated as what an individual earning the National Living Wage would earn for 416 hours of work (DWP, 2022^[42]).

contact information, detailed information on formal qualifications and basic skills, employment histories, disability status, agreed restriction on job search or training activities, career goals and job preferences, as well as additional comments from the individual action plan. In addition to the data shared at the outset, upon a client's referral, there is a "warm" handover during which a counsellor from DWP, a counsellor from the private provider and the jobseeker meet together. This can facilitate the exchange of additional information between DWP and the outside providers.

In addition to the information provided upon referral, providers are notified by DWP of important client developments relevant for providing services to their clients. The system used by DWP enables case tracking between DWP and the outside providers. This includes information on whether an individual has new claim for income support (universal credit), changes affecting the client's work-related requirements (e.g., jury service, civic duties, domestic emergency, easements for domestic abuse or violence), or other relevant changes to their personal situation (moving abroad, sickness, imprisonment or death).

After a provider has finished working with a client, no transfer of personal information on the client is mandated by DWP. In other words, data sharing for DWP to receive information from outside providers on individual cases after referral is not yet in place. This limits the information available to DWP in instances where a client returns to DWP in another unemployment spell.

Outside providers are also required to report only a limited information about service provision at the client level to DWP. The bulk of the information required for the case management is only accessible to the outside provider. Individual action plans outlining the client's planned activities and goals are in the provider's systems and not DWP, although DWP does get samples of how providers interact with individual clients. Performance managers from DWP may also conduct visits to providers and conduct the audits in person if necessary (although this may be done virtually as well, with the provider sharing the screen of the DWP staff member). Also, direct feedback on clients that is received by the outside providers from employers on a regular basis is not shared with DWP, unless the client is in breach of activation requirements. This lack of systematic data exchange also implies that conducting detailed evaluations to explain the underlying reasons for the performance of different providers is difficult.

DWP has access to a number of additional databases that it can use for research purposes which it does not yet use for operational purposes. For example, DWP staff can link its internal databases with the *Longitudinal Education Outcomes* database, which contains detailed information on educational progression and is maintained by the Department for Education. Furthermore, DWP is also able to access the data on criminal convictions for research purposes. However, DWP still needs to establish a legal basis for the use of such data for operational purposes in its day-to-day work with clients. This important topic – the legal basis for information exchange – is the subject of the next chapter.

3. Legal basis for information exchange in case study countries

Contracted-out employment services involve the processing of considerable amounts of personal information, including potentially sensitive information, by outside providers. This chapter discusses how the three case study countries in this report – Australia, Estonia and the United Kingdom – have addressed legal questions concerning the use of such information. Specifically, it examines the legal aspects concerning the processing and exchange of data, focusing particularly on the legal basis for data collection via user interfaces, data exchanges with external IT systems/databases (by databases and types of data) and data usage (how data are processed, by whom and for which purpose). It also discusses protocols and practices within each country to meet the requirements of national data protection regulations.

In terms of the comparability of the legal systems, among the three countries, Estonia is the most comparable to Sweden. As EU member states, they are both directly subject to GDPR. However, the legislative data privacy framework in the United Kingdom remains similar to what is in place in the EU despite the United Kingdom's departure from the EU. It remains based on the GDPR. Together with some changes pertaining to the practicalities of the United Kingdom's departure from the EU institutions, the legislation is now referred to as the "United Kingdom GDPR" and operates alongside the Data Protection Act 2018. While the data protection framework in Australia is quite different from the data protection framework in Europe and in Sweden specifically, the Australian Government's expertise in this field and the lessons learnt from their approach are valuable information for the purposes of this report.

3.1. Australia

Several laws regulate personal data processing and sharing in Australia in the context of public employment services. These include the Australian Privacy Act, the Social Security Act and the Data Availability and Transparency Act. According to the Social Security Act, certain information from jobseekers who are registered as unemployed or who are receiving income support from the public employment services will be shared with outside providers and used for the primary purposes of finding a job for them. Once the jobseekers get in touch with the outside providers, they are given the relevant information about how their data will be processed and they are told which information will be shared and under which legislation.

Any personal data requested from the jobseeker by the outside providers which is not explicitly covered by legal obligation is not mandatory. For example, during the initial profiling questionnaire (called *Job Seeker Snapshot*), several fields are optional: criminal convictions, status as an indigenous citizen, and presence of disabilities (DEWR, 2022^[33]). However, jobseekers are told that if they do not provide such information it can affect the services that can be provided. This principle also applies to other services provided from the government, as the right assistance cannot be provided without the information necessary for these purposes.

In practice, jobseeker consent is used not only for collecting data from jobseekers, but it also forms the lawful basis for personal data processing by the public employment services in Australia. At the moment this also applies where a jobseeker raises a complaint against the outside provider: whereas some jobseekers may prefer to keep their identity confidential, the Department may need to discuss with

them how this could affect management of the complaint, including any investigation and resolution. Consent is also being explored for the outside providers to be able to mirror some Government's systems and obtain the relevant information required for providing their services.

In order to promote better availability and use of government data, Australia recently adopted new legislation to clarify how government agencies are permitted to share and use data. Entered into force on 1 April 2022, the Data Availability and Transparency Act allows scheme entities to enter into data sharing agreements for a specified data sharing purpose and is intended to provide a clearer basis for the sharing of certain data between government agencies (it does not regulate the sharing of data with private providers). However, there is still some uncertainty about how this legislation will be implemented in practice given its relative novelty and lack of jurisprudence.

In contrast to EU law, the legal concepts of controller, joint controller and processor do not exist in the Australian data protection framework. Instead, DEWR imposes a set of obligations on the outside providers through a risk-based approach that comprises of several hundred controls known as Right Fit For Risk (for a more detailed discussion of this, see Section 4.1). Outside providers are required to maintain this accreditation to offer assurance of their IT security, covering storage, processing or communication of data related to delivering employment services and digital information. This includes all data and records associated with the programme delivery, with a particular focus on the sensitive information processed.

Jobseekers' personal information (including sensitive information) may be passed from DEWR on to other public entities in certain cases. Most notably, this includes agencies involved in the administration of employment services and income support payments and services. In addition, jobseeker's personal information may also be disclosed to other parties where the jobseeker has agreed, or where it is otherwise permitted by law, such as in cases of a court order.

Several data protection principles are observed in Australia. In terms of data minimisation, access to personal data is limited based on job roles. The data are also deidentified and identifiers are kept internally. And perhaps most importantly, private providers are required to submit to data security certification - a process which subjects them to data security protocols some of which are even stricter than those in place for DEWR (for more information, see Section 4.1).

3.2. Estonia

As an EU country, Estonia applies the GDPR when processing personal data, including exchanging data with other stakeholders and registers. Regardless of the channel used for data exchange (*X-road*, the self-service portal or encrypted emails), the exchange may only take place in case there is a basis in the legislation. The EUIF notes, however, that a statutory basis is not always entirely clear in relation to the personal data processing for specific tasks – there is the question of how detailed the regulation needs to be concerning specific tasks and data processing to fulfil these tasks. A continuous improvement process takes place in regulations to support effective and efficient use of data and better (digital) services for citizens, while ensuring data protection. In addition to such statutory bases, consent is used as a legal basis for ad hoc purposes such pilot projects (with recent examples including follow-up services to EUIF clients who become employed or person-centred special care service model in the local government involving multiple stakeholders). If a pilot programme is scaled up or implemented in full, then the legal basis for information exchange or processing is updated so that an individual's consent is no longer necessary as the legal basis.

The EUIF is the owner of the register of jobseekers and active labour market policies (*Töötuna ja tööotsijana arvel olevate isikute ning tööturuteenuste osutamise register*), which has been set up by law and includes data in personal form for the provision of a service to a jobseeker, and in pseudonymised or anonymised form for evidence-based policy making (analysis, evaluations, research). Keeping the data in

personal, pseudonymised, or anonymised form based on the tasks performed is in line with the data protection by design principle.

When exchanging data with private service providers, the EUIF generally enters into data processing agreements with them, i.e. it treats them as personal data processors. The data minimisation principle is observed when sharing data with external service providers, similarly to any other stakeholder. Hence, only the data that are needed to provide their service are shared. Thus, despite the rich data available through the X-road platform in principle, sometimes external providers will receive only the most basic information about their client.

3.3. United Kingdom

The lawful basis for personal data processing in the United Kingdom relies on public interest clauses relating to data protection. DWP and its outside providers in their Model Services Contract rely on Article 6(1)(e) of the United Kingdom GDPR as the legal basis for the processing of jobseekers' personal data. According to this basis, the "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". For special categories of personal data, they further rely on Article 9(2)(b) of the United Kingdom GDPR, whereby the "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by [the] law providing for appropriate safeguards for the fundamental rights and the interests of the data subject".

The status of DWP and the outside providers is regulated by a contract entered into entered into between both parties. According to this contract, DWP and the outside providers are either independent controllers or joint controllers under the United Kingdom GDPR. The parties are joint controllers in respect to the clients data that they share for providing the services to which they have joint access for the purposes of delivery of the services. For data they collect and process which are not jointly shared with DWP, they are considered individual controllers. There is no scenario whereby the outside providers would be the data processors for DWP.

Several data protection principles are observed by DWP. Apart from a clear lawful basis, which limits the scope of uses and individuals given access, the United Kingdom's system takes account of the need for data minimisation and data protection by design. Specifically, for measuring outcomes, outside providers are given access only to data that is strictly necessary to establish that the jobseeker's revenue threshold has been reached and that the outside provider is therefore entitled to remuneration. Outside providers are only informed in real-time about the jobseeker's reaching of the revenue threshold without being able to trace the actual earnings of the jobseeker in real time.

4. Addressing information protection risks in case study countries

To address data security concerns and implement the legal requirements described in the previous chapters in practice, all three case study countries in this report – Australia, Estonia and the United Kingdom – have adopted a set of information security management standards for outside providers. These standards are intended to mitigate specific risks associated with data sharing and ensure the confidentiality of private data. The countries have adopted different approaches, which reflect the different contexts in which they are applied. In the United Kingdom, with its model of large “prime contractors”, all providers are required to adhere to the extensive IT standards. A similar system is in place in Estonia, which has extensive data sharing across government entities – but this has arguably led to problems with adoption among outside users, with only a handful of PES contractors currently using the system. Estonia is currently moving more towards a more risk-based system. Such a system is in place in Australia, where an assessment process by the contracting authority determines a contractor’s level of information security risk. This assessment then dictates the level of detail in the information security management controls implemented.

In Sweden, the lack of a comparable certification system may represent a barrier to expanding the scale and scope of data sharing between various stakeholders. The government may be reluctant to share more administrative data given the potential risks associated with a data confidentiality breach and the uncertainty regarding private providers’ information security protocols. Given the presence of smaller providers in the Swedish system, Sweden may consider adopting a risk-based approach to the certification of providers, similar to what has been implemented in Australia.

4.1. Australia

Australia’s extensive experience with contracted-out employment services has led to a well-developed system of cooperation between the contracting authority, DEWR, and individual providers, which is reflected also in the area of digital cooperation. DEWR controls the risks around sharing information and buying services from providers with an auditing and IT-requirement system called *Right Fit For Risk* (RFFR). Although responsibility for information protection around the employment services ultimately lies with DEWR, RFFR is tool to share that responsibility with the providers and ensure that the risks are adequately addressed. RFFR accreditation requirements are based on a customised Information Security Management certification (ISO 27001) and a whole-of-business approach to IT security. To gain accreditation, providers must design and implement an information security management system to protect the sensitive information they hold.

The approach to the outside providers’ accountability is based on their size and the requirements imposed on them are made conditional on this factor, the nature of the data processed, and the type of programme delivered. Outside providers in small areas do not have the same resources as bigger providers, and their risk profile is considered lower due to the amount and nature of the data processed by them and the systems used. the majority of small providers process data on the government’s systems, reducing data flows and the amount of data exchanged. The Australian Government took this decision for the purposes of avoiding inequity among outside providers and avoiding a situation where jobseekers in remote areas would not be able to access the services.

The rules for getting access to sensitive information and to the program are same across all providers, but the level of scrutiny and confirmation of the capabilities vary based on the risk potential. Providers with an annual caseload of at least two thousand jobseekers must undergo ISO 27001 certification from an accredited independent assessor (DEWR, 2022^[44]). For providers with caseloads below this threshold, DEWR categorises them as either medium or low risk, based on a RFFR questionnaire and additional information obtained through an interview with the provider (DEWR, 2022^[45]). For small providers categorised as medium risk, this official audit is replaced with a self-assessment of the ISO 27001 requirements. For small providers classified as low risk providers, RFFR requires only management level assertion that sufficient security practices are in place.

RFFR is not a complete copy of the very extensive ISO 27001 standard. Instead, it focuses on eight main areas of information security. These eight areas have been defined by the Australian Cyber Security Centre to create what they term the *Essential 8 Maturity Model*. Table 4.1 list the areas of the model covered. Each area has several different concrete maturity levels. Large providers are expected to target Maturity Level 3, while smaller providers with less complex IT environments and less sensitive data in their possession may decide to target Maturity Level 2 or 1 (DEWR, 2022^[46]). The *Essential 8 Maturity Model* makes the controls as practical as possible and direct action to areas of most impact. In the model all maturity levels represent similar level of information protection capability. An organisation's job is to pick their target maturity level and then ensure all that all eight areas meet that level of criteria. This is to ensure that the most important information protection areas are addressed in similar fashion and ensure there are no essential weak points (ACSC, 2022^[47]).

Table 4.1. Essential 8 Maturity model focus areas

Area	Description
Application control	What is being done to prevent the execution of unauthorised software?
Patch applications	What is being done to identify and mitigate known security vulnerabilities in application software?
Configure Microsoft Office macro settings	What is being done to block untrusted macros?
User application hardening	What is being done to limit the potential for security vulnerabilities in user applications (focusing on application-specific security settings and removing unneeded functionality)?
Restrict administrative privileges	What is being done to limit actions taken by accounts with powerful access?
Patch operating systems	What is being done to identify and mitigate known security vulnerabilities in operating systems?
Multi-factor authentication	What is being done to protect against accounts being inappropriately accessed?
Regular backups	What is being done to maintain the availability of critical data and systems to allow your business to recover quickly if required?

Source: DEWR (2022^[48]).

As of October 2022, there were up to 779 individual control requirements, although only a subset are relevant for specific providers.¹⁴ Of these 779 controls, 98 related to areas covered by the “Essential 8” model. To give a sense for the level of detail in these controls, it is instructive to examine the excerpts from three of them (DEWR, 2022^[49]):

- Control 0240: SMS and messaging apps are not used to communicate sensitive or classified data.
- Control 0864: Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.

¹⁴ In fact, some of the controls are overlapping or mutually exclusive.

- Control 1576: If an organisation's systems or data are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified.

Before undergoing certification, providers are to examine their security risks and assess the applicability of the individual security controls to their specific circumstances. They are to then propose which controls are applicable to them.

Before the launch of *Workforce Australia*, several steps were taken to facilitate providers' adoption of the security management certification. DEWR instituted a special capacity building fund to reimburse eligible providers for some of the costs associated with obtaining IT security accreditation. Furthermore, in the initial tender process for *Workforce Australia* providers had an option to build their capabilities around information protection within the process. High risk providers had nine months after a successful bid to be certified by ISO 27001 capable auditor. Failing to pass the certification can lead to termination from the programs (DESE, 2021^[50]).

DEWR also has a system for accrediting the software that the private providers can use in their operations and which process client data. Called *Third Party Employment and Skills* systems, these are software solutions that are developed by private companies. As of October 2022, nine systems were accredited by DEWR (DEWR, 2022^[51]). Accreditation signifies that a system has met the requirements for protecting sensitive information but does not imply that DEWR endorses a specific system.

4.2. Estonia

In order to manage the risks in information protection, the Estonian PES has implemented an information security standard developed for the Estonian public sector. It is called ISKE - *InfoSüsteemide Kolmeastmeline Etaloniturbe* ("three-layered, front-line security of information systems"). The intention with ISKE is to ensure sufficient security levels for data processed in information systems. ISKE addresses the level of security in organizational, infrastructural, physical, and technical matters. ISKE is based on the German standard IT-Grundschutz, which is a methodology for identification and implementation of tasks and measures for IT security that used to be maintained by the German Federal Office for Information Security. ISKE consists of more than 1 000 security measures, but entities are subject to differing security requirements based on the databases they access and the information systems they use. ISKE classifies entities into three different categories of requirements.

The underlying framework behind ISKE, IT-Grundschutz, differs slightly by methodology compared to ISO 27001. Both IT-Grundschutz and ISO 27001 are standards that are highly recognized and adapted in the field of IT security. They both rely on the ISO 27001 framework, enabling organizations to ensure confidentiality, availability, and integrity of information (Myra Security GMBH, 2022^[52]). However, the Grundschutz system stopped being updated in 2018, meaning that the system standards may not adequately account for up-to-date IT threats.

Estonia is currently working to replace the ISKE system with a new standard which is to be implemented in 2024. In addition to accounting for up-to-date IT threats, Estonia intends to adopt a more risk-based approach which tailors the requirements to the level of risk, more along the lines of what has been adopted in Australia. The ISKE standard arguably imposes large compliance requirements which may be unreasonable for a smaller organisation, with the full requirements comprising almost 5 000 pages of text (Republic of Estonia Information System Authority, 2021^[53]). The changes are intended to facilitate more widespread adoption of the X-road data exchange platform.

Entities that are connected to state information systems are obliged to perform IT audits. Audits are performed from every two or four years, depending on the sensitivity of managed data. Audits can be assigned separately by the Ministry of Economic Affairs (Republic of Estonia Information System Authority, n.d.^[54]).

4.3. United Kingdom

Programmes such as *Restart* involve extensive amount of personal data sharing between the parties. To gain access to the PRaP and in extension to the program providers are contractually bound to follow DWP security policies and standards. This includes compliance with the ISO 27001 standard, although DWP does not require independent certification of compliance. During the bid phase, proof of the compliance against security policies needs to be submitted and is reviewed before the provider proof may be awarded a contract (DWP, 2022^[42]). DWP has the ability to limit provider access to PrAP until they have met the Department's security standards. Furthermore, audits are undertaken every 60 days to ensure the right staff at the provider have access to the system.

The DWP security policies and standards have several components (DWP, 2022^[55]), including:

- **Information Security Policy.** This relates to cyber and information security and is based on the ISO 27001 standards. This compliance is additional layer of risk mitigation on top of the information protection regulation like GDPR.
- **Acceptable Use Policy.** Relates to the behaviour of contractors and their employees relating to communication and usage of IT systems and personal data.
- **Cryptographic Key Management Policy.** Relates to the management of all cryptographic devices and materials including commercial encryption products.
- **Email policy.** Relates to acceptable use of email, including a description of the types of information that may not be transmitted via unencrypted means (bank account details, medical history/mental health issues, substance abuse, criminal records and benefit payment details).
- **Personnel Security Policy.** Relates to procedures concerning aspects such pre-employment checks, completion of Security E-Learning modules, procedures for departing staff and informing staff of the various security polices described in this section.

Additional information gathered by providers during the *Restart* programme from their clients is to be subject to the same controls as data provided to the contractors by DWP.

5. Lessons for Sweden based on experiences of other countries

Arbetsförmedlingen is undergoing an ambitious transformation which aims to give its clients a more active role in determining their pathways into employment. As part of wider changes that have been ongoing since 2015, Arbetsförmedlingen has been changing its delivery model of publicly-financed employment services to include more self-service tools for job-ready clients. It has also introduced the possibility for jobseekers who are referred to job brokerage services (*förmedlingsinsatser*) to choose their provider. To support these goals, Arbetsförmedlingen has invested heavily in its IT infrastructure, developing an effective self-service platform for jobseekers and an impressive array of digital tools. It also has plans to further develop its data exchange platforms and will continue to explore options for increased data exchange with outside employment services providers and other government registries. This is important given that the nature of the reform means that, in the future, information which previously would have been retained by Arbetsförmedlingen in-house will increasingly need to be shared and that obtaining data from additional registries will be even more important.

This final chapter provides assessments and recommendations relating to data exchange relevant to the reformed system. It begins by contrasting the situations from the three other countries studied: Australia, Estonia, and the United Kingdom. Drawing on specific lessons learned from these countries, it then discusses recommendations for improving information exchange in Sweden.

The case study countries offer interesting lessons to Sweden

In terms of its IT-capabilities, digital platforms and customer journeys, Australia shares the most similarities with Sweden. The Australian and Swedish authorities overseeing publicly-financed employment services have similar approaches to the use of digital tools and platforms in supplying services to their clients, referring some clients to self-service tools and others to outside providers. The comparison with Estonia provides an interesting example of the potential far-ranging impact of digital government transformation that has taken place in the country beginning in the 1990s. The central lessons from United Kingdom relate to the potential benefits of integrating income tax data into the operations of contracted-out employment services.

Both the Australian contracting authority, DEWR, and Arbetsförmedlingen share a similar digital strategy and roadmap. This makes Australia a useful benchmark and potential future knowledge sharing partner. The emphasis on the modern digital service development and lessons learned around it can be very valuable to Arbetsförmedlingen's own development. The fact that Australia – with its established track record in large-scale contracted-out employment services – has taken a similar approach in its IT infrastructure provides additional affirmation to Sweden's approach.

Australia's contracting authority has a long history of cooperating with employment services provider providers. DEWR know the provider landscape and have strong practices in place to cooperate with providers. This knowledge and cooperation opportunities have been built purposefully and have led to practises that are proven to work and produce value for all parties included. This experience with

providers and the similar digital strategy to Arbetsförmedlingen means the lessons learned relating to Australia's country example have the potential to be analysed further.

The Estonian government's digital transformation has shown in practice the potential for data sharing to increase efficiency in the public sector. By creating models where systems integration and dataflows become standard, public organisations have been able to produce services with high levels of automation and transparency. Furthermore, by providing a standardised distributed information exchange platform, the costs associated with having systems access different databases have been reduced significantly: the need for system-to-system integrations has been reduced due to the usage of the X-road technology.

Some aspects in the Estonian case that could be incorporated into the context of contracted-out employment services in Sweden, even though it would be unrealistic to propose the Estonian model as a solution for Arbetsförmedlingen's IT infrastructure and data management. Estonia's "once only" principle could be applied to data currently collected by Arbetsförmedlingen and its providers, with information exchange between the counterparts help lower the reporting burden of acquiring information and facilitate the work of all parties. Nevertheless, the Swedish government's initiative to create a common digital infrastructure for information sharing is a promising step in this direction (The Swedish Government, 2022^[14]).

The United Kingdom's DWP has invested sizable time and resources to facilitating the exchange of information in its contracted-out employment services operations. Its PRaP system has eliminated the need for significant amounts of manual work. It has also enabled more transparent ways of working, allowing providers to automatically track their clients. Interestingly, this increased data exchange has in fact resulted in higher levels of client privacy in certain respects – the integration of the data exchange into the platform, with providers notified when their clients pass certain milestones, means that providers can provide less intrusive follow-up support to clients.

Arbetsförmedlingen's technology stack and overall system architecture is modern and up to date, with continued investments necessary for a stable platform for future digital service development

Arbetsförmedlingen has the IT capabilities and agile development practices required to develop and sustain a modern digital platform. The current technology stack aims to provide enough abstraction layers for modern software development and supports mobility as well as reliability. Arbetsförmedlingen has a hybrid-ready technology stack, which means that the infrastructure is not bound by technology to the on-premises capacity services and will enable Arbetsförmedlingen to opt for cloud services in the future if the Swedish government were to change its policy about the use of such services. The use of a container platform and a robust integration layer is crucial for digital service platforms such as the one that is being built in Arbetsförmedlingen. In this set-up, the microservice architecture relies on self-contained units, each dedicated to a specific part of business capability and usually developed independently of each other. This leads to speed and reliance in case of changes in the business requirements. The communication and integration layer chosen by Arbetsförmedlingen to connect the microservices is an industry-leading software stack, providing it with a good position to succeed in its further IT developments.

Arbetsförmedlingen has made significant investments in technology and modern, agile ways of working to enable the development of its digital platforms. It has built custom digital service portals to host services for similar types of users and purposes. In these respects, it similar to Australia's contracting authority, DEWR. Both DEWR and Arbetsförmedlingen have both acquired modern IT-capabilities to enable this digital transformation. DEWR utilizes modern agile software development practices and public cloud services for the computing needs. Arbetsförmedlingen has an Scaled Agile Framework in place to support software development and, while the services themselves are hosted on-premises, computing services have been built with flexibility in mind. Arbetsförmedlingen's utilization container services and

flexible open-source solution are examples of building flexibility to on-premises solutions. These kinds of solutions enable maximum movement in case cloud-based capacity services become an option. They also provide the required additional abstraction layers between infrastructure services and application development which form the basis for swift modern digital service development.

The fact that Arbetsförmedlingen cannot make use of cloud-based solutions does not appear to be a limiting factor as long as it continues to invest in its on-premises capabilities. However, it is important that such investment in the underlying on-premises capacity services continues: the speed of modern software development is hard to match in the on-premises data centre service area without ongoing investments. More IT-capability and architecture decisions will need to be made as new requirements arise and the general modernization continues. These decisions should prioritise flexibility and suitability for modern digital service development.

Arbetsförmedlingen should embrace modern, agile ways of developing digital services to encompass the entire organization and not just the IT and digital service development teams within Arbetsförmedlingen

One of the main enablers of building new digital platform is to facilitate the needs of modern application development. This means that agile best practices need to be in place, with developers having access to flexible capacity services and entrusted with enough autonomy to build services effectively. In Australia, more than any other factor, modern development tools were mentioned by DEWR as one of the key enablers for the *Workforce Australia* platform. It is excellent to see Arbetsförmedlingen has enterprise-scale agile framework capabilities in place at least in part of the organisation.

Agile ways of working can help ensure that Arbetsförmedlingen makes full use of the extensive technical capabilities that it has acquired and reap the full benefits of these sizable investments. In 2021, Arbetsförmedlingen began using SAFe, a widely used and well-suited framework for this purpose. At the same time, the specific framework employed is not as important as commitment to the cultural change these frameworks require.

Arbetsförmedlingen should fully commit to the agile ways of working for all parties involved in the realization of its digital services. This should include not only the IT and digital service development teams, but also other parts of the organization. Arbetsförmedlingen should also increase the involvement of the end-users in the development of its digital platforms and services. For example, they could be actively involved in the design of the development roadmaps or be consulted as beta testers before the rollout of new services. One area where the outside providers should be directly involved includes the development of data exchange integrations (APIs).

Arbetsförmedlingen should be granted increased access to external administrative data sources instead of relying heavily on information collected from customers

Sweden has enacted legislative changes to give Arbetsförmedlingen a legal basis for increased access to external administrative sources. From 1 December 2022, Arbetsförmedlingen will have access to the Swedish tax authority data to measure employment outcomes. This is a welcome development and will hopefully allow Arbetsförmedlingen to better follow-up the activities of the outside providers, improving the *betyg* grading model for rating outside providers and the accuracy of payments made to suppliers, as well as enabling better labour market statistics. At the same time, access to administrative data bases could be further expanded to incorporate additional relevant sources. Most prominently, this includes information necessary to measure educational outcomes of clients.

The country case studies have shown the numerous potential benefits of greater access to external administrative data sources. In the United Kingdom, access to tax data sources has enabled a provider

compensation model based on employment milestones. Access to program participants tax records has created a solution where compensation payments and their management and monitoring can be highly automated and near real time. In Estonia the digital landscape is based on the principle that once data are shared to a public institution the responsibility for providing the data is no longer at the citizen but must be shared between organizations. The Estonian model enables real time data sharing between actors creating opportunities to streamline processes and provides a richer informational foundation for implementing new technologies, such as AI-based decision making tools. Arbetsförmedlingen currently works almost exclusively with data collected from clients or recorded by caseworkers, but significant efficiency benefits will be available if more governmental data sources could be used enrich the data models. The assessment that information exchange between government agencies should be increased is also highlighted in a recent government inquiry (The Swedish Government, 2022^[56]) which argues that “the current secrecy override provisions do not permit sufficient exchange of information of importance for another public authority” (p. 24). The inquiry supports expanding the scope of automatic data exchange, including information pertaining to migration and education.

Discussions relating to data privacy should recognise that giving Arbetsförmedlingen increased access to outside administrative data sources can, paradoxically, facilitate the principles of data minimisation and data protection by design. For example, in system similar to that used in the United Kingdom’s Restart programme, outside providers could be notified by Arbetsförmedlingen when their clients have passed certain employment or educational milestones.

Increasing data sharing between Arbetsförmedlingen and employment services providers – possibly with the use of consent workflows – would decrease data reporting burdens while also facilitating monitoring and research of providers’ activities

Relatively few data are currently shared between the actors in contracted-out employment services in Sweden. The current state of information exchange means both contractors and Arbetsförmedlingen collect and store similar data from clients. This has led to a situation of parallel data flows and separate data silos. In addition to imposing a data burden on all parties involved – jobseekers, private providers and Arbetsförmedlingen – this multiplication of datasets increases the risk of data quality discrepancy and duplicate entities. For example, changes in client’s personal or employment status are not necessarily updated in all the databases held by various stakeholders. This has shown to be a problem in practice in Sweden with Arbetsförmedlingen’s online platform for where employers can search for workers: consultations with stakeholders indicate that the portal is of limited use in practice, partly due to an abundance of outdated information on jobseekers. The problem of a lack data exchange is magnified if clients decide to switch providers during their unemployment spell: they must again report information which had previously also been collected (possibly by both Arbetsförmedlingen and the previous employment services provider).

Facilitating data exchange from outside providers to Arbetsförmedlingen could also streamline the process of obtaining data from providers on their activities with clients. Currently, such data need to be inputted on by providers on an ad hoc basis specifically for reporting purposes. However, with the development of automated data exchange, this could conceivably be integrated into the normal business processes of the providers This could minimise the reporting burden imposed on providers while also enriching the data available for monitoring providers, to ensure that they are fulfilling their contractual minimum services requirements. It could also be used for research purposes, for example, to examine the relative efficiency of more intensive service provision across different jobseeker profiles.

One potential solution to the legal challenges relating to data sharing would be to create so-called consent workflows, similar to what is in place for certain data used by providers in Australia. By enabling consent, clients could approve and grant data transfers between parties in contracted-out employment

services. In such a system, data transfers, integration management and monitoring could be done on both platform and machine-to-machine levels. Consent workflows would allow for more automation and a better user experience for clients. The data accumulated on jobseekers and the activities undertaken to support them could be shared with Arbetsförmedlingen.

Cooperating closely with private providers could facilitate Arbetsförmedlingen's implementation of its digital integration and co-operation roadmap and allow it to become a key enabler for the digital development of employment services

Providers of contracted-out employment services in Sweden differ quite significantly in their size and technical capabilities. The current co-operation platforms provided by Arbetsförmedlingen for employment services are online-based digital platforms, with some possibilities for integrations through APIs. For the moment providers can use APIs only for obtaining information from Arbetsförmedlingen. Data that is to be sent for Arbetsförmedlingen involves a manual process via the digital platform or, as is currently the case for some sensitive information, through regular mail.

Arbetsförmedlingen's digital integration and co-operation roadmap consists of three steps:

- i.) creating a digital platform for jobseekers, employment services providers and employers,
- ii.) developing Arbetsförmedlingen's APIs, and
- iii.) a broader integration platform for employment services.

The current digital platform is suited for smaller actors with lesser needs for integrations and data transfers. Larger actors have made investments in their own systems and IT architectures, potentially reaching the level of technical capabilities where extended integrations could already be implemented.

In the Australian model DEWR has taken a role as an enabler for digital co-operation between providers and the public entities. Arbetsförmedlingen should consider further examining the Australian practises in creating a shared digital landscape for providing employment services with private providers. Increasing co-operation between Arbetsförmedlingen and private providers could help enable process development, as well as enhance data quality through common data models and modern integration platforms.

Arbetsförmedlingen should intensify its co-operation with private providers as it begins its API and integration development. Arbetsförmedlingen could take a similar role as its counterpart in Australia, where DEWR has taken the role as an enabler for digital co-operation in employment services.

Arbetsförmedlingen's plans for implementing solutions to consolidate key data providing context for Arbetsförmedlingen operations – master data management – should also take into account that more data may eventually be automatically exchanged with private providers

Arbetsförmedlingen is currently in the process of implementing technologies for master data management, which enables consistent and up-to-date information on important aspects of Arbetsförmedlingen's operations such who is currently registered as unemployed. Arbetsförmedlingen's architecture is a combination of legacy systems and modern solutions. It is not uncommon that master data management implementations face difficulties when data exports from legacy systems do not align with data models intended for master data management systems. This often requires solutions such as creating data models by exporting data from legacy systems and rearranging them through data warehousing. Co-operation with providers should be taken into consideration when working on data models or data taxonomy for contracted-out employment services. This would benefit both parties when

dealing with the same or similar datasets, by creating comparable data and a common language for describing data.

The Estonian country comparison presents a good example of a best practice in this regard. The unique way of sharing data between all public sector actors is enabled by the X-road integration technology. The solution adopted by Estonia to share data leads all actors to identify data in a common way: they share similar data taxonomy. This lowers the marginal costs associated with establishing an additional data exchange. Arbetsförmedlingen's cooperation with Sweden's Agency for Digital Government, DIGG, has the potential to lead to similar synergies in the transfer of information in Sweden.

Consider introducing mandatory risk-based information security management standards

Contracted-out employment services involve the use of significant amounts of personal and sensitive information. Ensuring data privacy is an important priority for the Swedish government and there are extensive regulations in place to safeguard personal data. However, relying on only data protection agreements and legislative requirements may not sufficiently address data security risks in practice. Arbetsförmedlingen should consider using certification or auditing practises to ensure information protection and other information technology related risks are properly addressed across the delivery chain. In all the comparison countries in this assessment, some level of information security management standards are in place. These standards are generally based on the ISO 270001 standard, with modifications based on the information protection and information technology security guidelines of each countries public sector. Compliance with these standards is also audited.

Given the presence of smaller providers in the Swedish system, Sweden could adopt a risk-based approach to the certification of providers similar to what has been adopted in Australia. Under such a system, larger providers would be given direct access to a wider array of personal data and could be required to meet the more stringent information security requirements reflecting their greater level of risk. The specific security requirements imposed on outside providers may be determined by the size of the outside provider, the systems used to process personal data and the nature and amount of personal data processed

Adopting different security standards in accordance with risk is not inconsistent with data privacy legislation, assuming all providers abide by the minimum obligations mandated by the GDPR and the Swedish national law. In GDPR, no specific requirements are imposed regarding the implementation of data confidentiality measures.¹⁵ Subject to the GDPR minimum requirements and any limitations laid down by national law, Arbetsförmedlingen can define the security measures required to each outside provider based on an assessment of the associated risk.

Implementing such security standards in practice could be done either by adding such clauses to Arbetsförmedlingen's contracts with outside providers or through legislative changes. The first option would involve phasing in such requirements into the contracts Arbetsförmedlingen has with its providers, with clauses stipulating the conditions under which a provider would be subject to which requirements. The second option would involve expanding Arbetsförmedlingen regulatory capacity that

¹⁵ Article 32 GDPR mandates the implementation of technical and organisational measures which ensure a level of security appropriate to the risk, including as a minimum "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing".

would allow them to define which security measures are appropriate for different categories of providers, based on relevant risk factors.

The adoption of any such requirements would ideally also be conducted in consultation with the outside providers and allow for a gradual adoption. Involving outside providers in the process and asking them for their views before the controls are made mandatory, together with providing a clear identification and definition of the outcomes expected, may help facilitate their adoption. The adoption itself could be a multi-stage process, imposing critical controls for immediate implementation and additional controls that could be applied afterwards throughout a maturity process. Such approaches have been adopted in Australia, where consultations with individual providers indicated that compliance costs are often substantial, particularly for smaller providers. Many of the larger providers, on the other hand, had implemented many of the controls even before they were mandated by the government. Thus, being flexible and including exemptions for smaller providers – as well as providing funds to help offset compliance costs, as Australia did – can be beneficial to ensure potential risks around information technology do not represent an undue entry barrier for providers in the employment services market.

Clarify some legal aspects regarding data sharing, including whether employment services providers should be considered “joint controllers” of personal data

Arbetsförmedlingen’s current interpretation of the legal status of outside providers implies that providers are limited in terms of what services they can offer to jobseekers from a legal perspective. At present, outside providers are considered “data processors” of their clients’ personal data. This implies that they can only act on Arbetsförmedlingen’s instructions, without flexibility in terms of the activities carried out and the decisions taken by them in the provision of their services. In a controller-processor relationship, the instructions given by the controller with regards to the processing of personal data need to be specific and detailed. This involves describing precisely not only the rights and obligations of each party but also the subject-matter, nature and purpose of the processing, the type of personal data processed and the categories of data subjects involved (Article 28 GDPR and EDPB Guidelines 07/2020). General and vague instructions would not be compliant with the data protection framework and would imply a legal risk for Arbetsförmedlingen, who would remain liable as a controller for the data processed by outside providers on their behalf as processors. Accordingly, defining outside providers as joint controllers would be a more suitable approach to provide a solid legal basis for outside providers’ activities with their clients.¹⁶ While legislative changes have clarified and expanded the scope of client data that outside providers may legally process (including sensitive personal data), these changes have not addressed the question of whether outside providers are considered data processors or (joint) controllers.

In addition, Arbetsförmedlingen could take further steps to clarify important legal aspects of data protection pertaining to outside providers should they be classified as joint controllers. This would need to cover the following:

- **Implementation of general data protection principles.** A joint controller agreement could clearly define the data that can be shared pursuant to the Ordinance (2002: 623), and the purposes for which the data can be processed, in compliance with the Act (2002: 546). This would, for example, help address Arbetsförmedlingen’s concerns about outside providers possibly using the data to

¹⁶Following EDPB Guidelines 07/2020 on the concepts on controller and processor in the GDPR and the case-law of the CJEU, Arbetsförmedlingen and outside providers should be considered *joint* controllers – as opposed to simply controllers – because of their joint participation through converging decisions when handling clients. While Arbetsförmedlingen manages and monitors unemployment benefit and the initial registration of the jobseekers, carries out jobseeker’s profiling, evaluates performance and results and sets and addresses the payments to outside providers, outside providers help and prepare the jobseekers to access the labour market. The processing would not be possible without both parties’ participation as the processing by each party is inextricably linked.

build an AI model outside the agreement. Where there is no other valid lawful basis to process personal data and where this is allowed by Swedish national law, Arbetsförmedlingen could note to outside providers that consent may be used as a lawful basis for collecting information from jobseekers.

- **Response to data subjects' requests.** GDPR contains stipulations for individuals to make requests concerning their personal data.¹⁷ While a recommended approach is that each party takes responsibility over the requests they receive and the provision of information about their data processing activities to the data subjects, other alternatives may be explored. For example, in the United Kingdom the outside provider is solely responsible for taking all the necessary steps to fulfil data subjects rights exercise requests and for the parties' compliance with all duties to provide information to jobseekers under GDPR Articles 13 and 14.
- Notification of a personal data breach to the supervisory authority and to the data subject.¹⁸
- **Data Protection Impact Assessments.** The parties should provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required, for example in relation to the outside provider's use of AI in processing their clients' data.
- **The use of third-party software used to process personal data by the outside providers.** Arbetsförmedlingen has indicated that the use of third-party systems by outside providers is one of their main challenges for the adoption of more extensive data sharing. Whereas they would like to provide via APIs to share data with the outside providers, they need to ensure the at the personal data will be adequately protected by any third parties involved in the processing of this data. To address this issue, Arbetsförmedlingen may consider requiring outside providers to confirm that they have entered into a Data Processing Agreement with every third-party processor they use.¹⁹ Alternatively, Arbetsförmedlingen may also adopt a system similar to what DEWR has in place, which accredits the software that the private providers can for processing client data.
- **Transfers of data to third countries.** Arbetsförmedlingen should impose on outside providers the obligation to confirm the actual third countries where they may process the personal data.²⁰

To facilitate research relating to contracted-out employment services, consider expanding the lawful basis to enable the use of other administrative databases in-house and carefully consider providers' reporting requirements

The rich labour market data available in Sweden, including linked data from numerous administrative sources, have formed the foundation for a rich evidence base to inform policymaking in Sweden as well as to examine important questions in the field of labour economics more generally. Research using individual-level administrative data is currently conducted either i)

¹⁷ The transparency duties to provide the data subjects with the relevant information are outlined in Articles 13 and 14 GDPR, that is, information about the controllers and how the data will be processed, including, inter alia: controllers' and, where applicable, controller representative's and controller data protection officer's contact details; categories of personal data concerned; purpose and legal bases of processing, recipients or category of recipients of personal data and information about international data transfers, data retention periods and data subject rights

¹⁸ It should be noted that Articles 33 and 34 of GDPR, that is, data breach reporting and communication obligations, do not apply in the case of personal data incidents that must be reported according to the Security Protection Act (2018:585), notified according to the Security Protection Act (2019:109) in the Riksdag and its authorities, or is reported or notified according to regulations that have been issued in connection with those laws.

¹⁹ Article 28 GDPR and Sections 7.f and 13.c of the Ordinance (2002: 623) are applicable here.

²⁰ Outside providers should confirm that EU Commission Standard Contractual Clauses (4 June 2021) are used where relevant, that a Data Transfer Impact Assessment has been performed to assess any risks that the transfer may involve, and that any required additional security and mitigation measures have been put in place.

through databases available internally at Arbetsförmedlingen, ii) using the LISA database provided by Statistics Sweden, the national statistical agency, or iii) through a database accessible by IFAU, Sweden's Institute for Evaluation of Labour Market and Education Policy. Two important questions relating to research are examined below. First, ensuring that detailed data are available for research that is timely enough to inform decisions about ongoing programmes, and second, ensuring that useful data exists on the services and activities of the employment services providers and that it is available to researchers.

To enable timely research into ongoing programmes, Arbetsförmedlingen would ideally have in-house access to additional databases for research purposes. The existing data used internally for research purposes has the benefit of being up-to-date, but relies almost exclusively on data collected from jobseekers, counsellors or outside employment services providers. The addition of earnings data from the Swedish tax authorities is a welcome development, but further steps could be taken to widen the scope of data available for research purposes internally, including e.g. data on education, household composition, disability status, and data from municipalities. Such increased access could be accompanied by stronger data protection measures for the use of such data – similar to what is implemented by Statistics Sweden – including the pseudonymisation of personal identifiers for research purposes. Such a database would open a number of possibilities for expanding the evidence base. For example, automatic impact evaluations of labour market policies could be part of Arbetsförmedlingen's key performance indicators in the future. The German PES has been using a semi-automatic tool called TrEffeR for CIEs already since 2008, the Estonian PES adopted a similar fully automatic tool just recently (OECD, 2022^[57]), and Slovakia has a webpage where automatic reports of ALMP impact evaluation results are periodically published (LMEvidence.sav.sk, 2022^[58]).

Ensuring that useful data exist on the services and activities of the employment services providers requires careful consideration to the reporting requirements and guidance to the providers for filing them. Currently, research into the activities of providers faces some challenges relating to how data are reported by providers. For example, the existing interface used by providers for reporting to Arbetsförmedlingen on the services they provide to jobseekers, for example, allows for reporting in increments of 60 minutes. This means that providers cannot report smaller intervals. Furthermore, providers appear to inconsistently filing the information required on the reports, making it difficult to analyse which types of services are more beneficial for different types of jobseekers. Arbetsförmedlingen is addressing the latter challenge through better guidance for the providers on how to file the reports. Decisions on which information providers are obligated to report, however, should balance the need for monitoring and research, on the one hand, with the administrative burden this imposes on the providers. In the longer term, such trade-offs will ideally be addressed through streamlined information exchange, with the automated exchange of information facilitating the work of all the interested stakeholders.

References

- (n.a.) (n.d.), *The Sw.* [63]
- ACSC (2022), *Essential Eight Maturity Model*, <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model> (accessed on 2022). [47]
- Arbetsförmedlingen (2022), *Our mission*, <https://arbetsformedlingen.se/> (accessed on 2022). [17]
- Arbetsförmedlingen (2022), *Collaboration Portal*, <https://arbetsformedlingense.force.com/apiportal/s/?language=sv> (accessed on 2022). [19]
- Arbetsförmedlingen (2022), *How we assess how quickly you can get a job and what support you need*, <https://arbetsformedlingen.se/other-languages/english-engelska/anvanda-webbplatsen/bedomning-och-profilering> (accessed on 15 September 2022). [15]
- Arbetsförmedlingen (2022), *Så hanterar vi dina personuppgifter*, <https://arbetsformedlingen.se/om-webbplatsen/juridisk-information/sa-hanterar-vi-dina-personuppgifter> (accessed on 29 August 2022). [10]
- Arbetsförmedlingen (2022), *Vi förbereder en ny myndighet*, <https://arbetsformedlingen.se/om-oss/var-verksamhet/nu-och-da/vi-forbereder-en-ny-myndighet> (accessed on 30 August 2022). [2]
- Azzopardi, D. et al. (2020), “Seizing the productive potential of digital change in Estonia”, *OECD Economics Department Working Papers*, No. 1639, OECD Publishing, Paris, <https://doi.org/10.1787/999c7d5a-en>. [34]
- Benmarker, H. et al. (2021), “Krom – erfarenheter från en ny matchningstjänst med fristående leverantörer inom arbetsmarknadspolitiken [Krom – experiences from a new matching service with independent providers in labour market policy]”, *IFAU Report*, Vol. 7, <https://www.ifau.se/Forskning/Publikationer/Rapporter/20212/krom--erfarenheter-fran-en-ny-matchningstjanst-med-fristaende-leverantorer-inom-arbetsmarknadspolitiken/>. [28]
- Benmarker, H., O. Skans and U. Vikman (2013), “Workfare for the old and long-term unemployed”, *Labour Economics*, Vol. 25, pp. 25-34, <https://doi.org/10.1016/j.labeco.2013.04.008>. [26]
- Carlsson, S., J. Román and J. Phalén (2022), *Uppdrag med anledning av en reformerad arbetsmarknadspolitisk verksamhet Lägesbeskrivning den 3 oktober 2022*, Arbetsförmedlingen, Stockholm. [9]

- Cederlöf, J., M. Söderström and J. Vikström (2021), "What makes a good caseworker?", *IFAU Report*, Vol. 9, <https://www.ifau.se/globalassets/pdf/se/2021/wp-2021-9-what-makes-a-good-caseworker.pdf>. [24]
- Dahlberg, M. et al. (2020), "Labor Market Integration of Low-Educated Refugees: RCT Evidence from an Ambitious Integration Program in Sweden", *IFN Working Paper No. 1372*, <https://www.econstor.eu/handle/10419/240515>. [27]
- Department of Education (2022), *Changes to the Department of Education, Skills and Employment*, <https://www.education.gov.au/about-us/announcements/dese-changes> (accessed on 2022). [29]
- DESE (2022), *Workforce Australia – information for providers – factsheet*, <https://www.dese.gov.au/workforce-australia/resources/workforce-australia-information-providers-factsheet> (accessed on 2022). [31]
- DESE (2022), *Workforce Australia information for individuals*, <https://www.workforceaustralia.gov.au/individuals/coaching/how-to/workforce-australia/factsheet> (accessed on 2022). [30]
- DESE (2021), *Request for Proposal for the New Employment Services Model 2022*, <https://tenders.employment.gov.au/tenders/75899c03-930f-ec11-b6e6-00224815762f/> (accessed on 2022). [50]
- DEWR (2022), *Accredited Third Party Employment and Skills (TPES) Systems*, <https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation/accredited-third-party-employment-and-skills-tpes-systems> (accessed on 10 October 2022). [51]
- DEWR (2022), *ISO 27001 and Right Fit For Risk (RFFR) - issues to avoid*, <https://www.dese.gov.au/download/13646/iso-27001-and-right-fit-risk-rffr-issues-avoid/27362/document/pdf/en>. [46]
- DEWR (2022), *Job Seeker Snapshot Overview*, <https://www.dewr.gov.au/download/14003/job-seeker-snapshot-overview/27999/document/pdf/en>. [33]
- DEWR (2022), *Provider classification for accreditation*, <https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation/provider-classification-accreditation> (accessed on 2022). [44]
- DEWR (2022), *RFFR Statement of Applicability (SoA) Template*, <https://www.dewr.gov.au/download/13665/soa-template-ism-iso-map/30668/document/xlsx>. [49]
- DEWR (2022), *Right Fit For Risk (RFFR) Questionnaire*, <https://www.dewr.gov.au/download/13788/rffr-questionnaire/30048/document/docx/en>. [45]
- DEWR (2022), *Scope template*, <https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation/resources/right-fit-risk-rffr-scope-template> (accessed on 14 October 2022). [48]
- DSS (2022), *Job Seeker Classification Instrument*, https://www.dss.gov.au/sites/default/files/documents/08_2022/job-seeker-classification-instrument-guidelines-v-14.pdf. [32]
- DWP (2022), *DWP procurement: security policies and standards*, <https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards> (accessed on 15 October 2022). [55]

- DWP (2022), *Restart Scheme provider guidance*, [42]
<https://www.gov.uk/government/publications/restart-provider-guidance> (accessed on 2022).
- EDPB (2020), *Guidelines 05/2020 on consent under Regulation 2016/679*, [16]
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
- E-Estonia Guide (2022), *Story - e-Estonia*, <https://e-estonia.com/story/>. [35]
- Enterprise Estonia (2021), *AI to help the Estonian unemployed*, <https://e-estonia.com/ai-to-help-serve-the-estonian-unemployed/> (accessed on 25 August 2022). [39]
- European Commission, D. and W. Pieterston (2020), *Digital technologies and advanced analytics in PES : thematic paper*, Publications Office, <https://doi.org/10.2767/371065>. [38]
- Foster, S. et al. (2014), *Work Programme Evaluation: Operation of the commissioning model, finance and programme delivery*, [41]
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/425301/rr893-report.pdf.
- GOV.UK (2022), *Find a job*, <https://findajob.dwp.gov.uk/> (accessed on 2022). [43]
- Hopsworks (2022), *Hopsworks Documentation*, <https://docs.hopsworks.ai/3.0/> (accessed on 2022). [20]
- Ilves, L. (2021), *e-Estonia guide*, https://e-estonia.com/wp-content/uploads/eestonia_guide_a5_220823_rgb.pdf (accessed on 29 August 2022). [36]
- JobTech Development (2022), *Making a stronger labour market through collaboration and open data*, <https://jobtechdev.se/en/about-jobtech-development> (accessed on 2022). [18]
- Langenbucher, K. and M. Vodopivec (2022), "Paying for results: Contracting out employment services through outcome-based payment schemes in OECD countries", *OECD Social, Employment and Migration Working Papers*, No. 267, OECD Publishing, Paris, <https://doi.org/10.1787/c6392a59-en>. [3]
- LMEvidence.sav.sk (2022), , http://www.lmevidence.sav.sk/?page_id=270 (accessed on 10 October 2022). [58]
- Ministry of Employment (2021), *Vissa lagförslag med anledning av en reformerad arbetsmarknadspolitisk verksamhet [Some legislative proposals related to a reformed labour market policy activity]*, Ministry of Employment, Stockholm. [1]
- Möttus, I. (2022), *Data exchange with service providers*, Eesti Töötukassa. [40]
- Myra Security GmbH (2022), *ISO 27001 vs. ISO 27001 based on IT-Grundschutz*, [52]
<https://www.myrasecurity.com/en/iso-27001-vs-iso-27001it-baseline-protection/> (accessed on 17 September 2022).
- OECD (2022), *Harnessing digitalisation in Public Employment Services to connect people with jobs*, OECD Publishing, Paris, <https://oe.cd/digitalPES>. [57]
- OECD (2019), *Unlocking the Digital Economy – A Guide to Implementing Application Programming Interfaces in Government*, OECD, <https://www.oecd.org/ctp/unlocking-the-digital-economy-guide-to-implementing-application-programming-interfaces-in-government.htm>. [59]

- Pillai, S. et al. (2021), *Magic Quadrant for Full Life Cycle API Management*, Gartner. [21]
- Rashid, N. and D. Eaves (2020), *Deploying the Once-Only Policy: A Privacy-Enhancing Guide for Policymakers and Civil Society Actors*, <https://ash.harvard.edu/files/ash/files/deploying-once-only-policy.pdf>. [61]
- Republic of Estonia Information System Authority (2022), *Data Exchange Layer X-tee*, <https://www.ria.ee/en/state-information-system/x-tee.html> (accessed on 17 October 2022). [62]
- Republic of Estonia Information System Authority (2022), *Data Exchange Layer X-tee*, <https://www.ria.ee/en/state-information-system/x-tee.html> (accessed on 2022). [37]
- Republic of Estonia Information System Authority (2021), *RIS newsletter March 2021*, <https://www.ria.ee/et/riigi-infosusteem/infokiri/ris-infokiri-marts-2021.html> (accessed on 17 October 2020). [53]
- Republic of Estonia Information System Authority (n.d.), *Estonian Security System Overview*, https://www.ria.ee/sites/default/files/content-editors/ISKE/iske_eng.pdf (accessed on 29 August 2022). [54]
- Scaled Agile (2021), *Welcome to Scaled Agile Framework® 5!*, <https://www.scaledagileframework.com/about/> (accessed on 2022). [22]
- Statistics Sweden (2022), *Longitudinal integrated database for health insurance and labour market studies (LISA)*, <https://www.scb.se/en/services/ordering-data-and-statistics/ordering-microdata/vilka-mikrodata-finns/longitudinella-register/longitudinal-integrated-database-for-health-insurance-and-labour-market-studies-lisa/> (accessed on 20 September 2022). [23]
- Sveriges Riksdag (2022), *Förbättrade förutsättningar för den arbetsmarknadspolitiska verksamheten - Arbetsmarknadsutskottets betänkande 2021/22:AU15*, Sveriges Riksdag, Stockholm, <https://data.riksdagen.se/fil/294D0395-F9E4-4A1F-B96B-4E6BEFBA0934> (accessed on 16 September 2022). [8]
- Sveriges Riksdag (2022), *Förordning (2022:811) med instruktion för Arbetsförmedlingen*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2022811-med-instruktion-for_sfs-2022-811 (accessed on 12 September 2022). [6]
- Sveriges Riksdag (2022), *Förordning (2022:812) om förmedlingsinsatser*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2022812-om-formedlingsinsatser_sfs-2022-812 (accessed on 12 September 2022). [7]
- The Swedish Government (2022), *Förbättrade förutsättningar för den arbetsmarknadspolitiska verksamheten [Improved conditions for labour market policy activities]- Proposition 2021/22:216*, https://www.riksdagen.se/sv/dokument-lagar/dokument/proposition/forbatttrade-forutsattningar-for-den_H903216. [13]
- The Swedish Government (2022), *Förbättrade förutsättningar för den arbetsmarknadspolitiska verksamheten*, <https://www.regeringen.se/rattsliga-dokument/proposition/2022/04/prop.-202122216/> (accessed on 12 September 2022). [4]

- The Swedish Government (2022), *Förordning om ändring i förordningen (2000:628) om den arbetsmarknadspolitiska verksamheten - SFS 2022:1245*, <https://svenskförfattningssamling.se/sites/default/files/sfs/2022-07/SFS2022-1245.pdf>. [11]
- The Swedish Government (2022), *Förordning om ändring i förordningen (2000:628) om den arbetsmarknadspolitiska verksamheten - SFS 2022:1435*, <https://svenskförfattningssamling.se/sites/default/files/sfs/2022-10/SFS2022-1435.pdf>. [12]
- The Swedish Government (2022), *Uppdrag att fortsätta etableringen av en förvaltningsgemensam digital infrastruktur för informationsutbyte*, <https://www.regeringen.se/regeringsuppdrag/2022/01/uppdrag-att-fortsatta-etableringen-av-en-forvaltningsgemensam-digital-infrastruktur-for-informationsutbyte/>. [14]
- The Swedish Government (2022), *Uppdrag med anledning av en reformerad arbetsmarknadspolitisk verksamhet*, <https://www.regeringen.se/regeringsuppdrag/2022/06/uppdrag-med-anledning-av-en-reformerad-arbetsmarknadspolitisk-verksamhet/> (accessed on 10 October 2022). [5]
- The Swedish Government (2022), *Utökat informationsutbyte [Expanded exchange of information] - Ds 2022:13*, <https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2022/07/ds-202213/>. [56]
- UK Government (2022), *Tell Us Once*, <https://www.gov.uk/after-a-death/organisations-you-need-to-contact-and-tell-us-once> (accessed on 15 October 2022). [60]
- van den Berg, G. and J. Vikström (2014), "Monitoring Job Offer Decisions, Punishments, Exit to Work, and Job Quality", *The Scandinavian Journal of Economics*, Vol. 116/2, pp. 284-334, <https://doi.org/10.1111/sjoe.12051>. [25]