Universiteit Utrecht

System Risk Indication

An Assessment of the Dutch Anti-Fraud System in the Context of Data Protection and Profiling

***

31 March 2016

Authors:

Steven van Dalen
Alexander Gilder
Eric Hooydonk
Marc Ponsen

Supervisors:

Dr Brianne McGonigle Leyh
Mistale Taylor LLM

Executive Summary

This report presents the main findings of a research project into System Risk Indication (SyRI), which is an anti-fraud detection system. Governmental institutions in the Netherlands may cooperate in so-called intervention teams to detect tax and allowance fraud and non-compliance with labour regulations. They may request to use SyRI for this purpose. This report answers two research questions:

1. To what extent does SyRI comply with data protection principles based on Council of Europe and European Union law?
2. What are the risks that follow from (partial) non-compliance with data protection principles based on Council of Europe and European Union law?

The legal framework consisting of Council of Europe (CoE) and European Union (EU) law form the basis for the assessment framework. The assessment framework consists of five principles derived from CoE and EU legislation and case law. These principles are:

1. the principle of lawful processing;
2. the principle of purpose specification and limitation;
3. data quality principles;
4. the principle of fair processing;
5. the principle of accountability.

Although the use of SyRI constitutes an interference with the right to respect for private and family life and a limitation of the enjoyment of this same right and of the right to protection of personal data, it seems that this interference is justified and that this limitation is lawful. This in turn leads to the conclusion that the use of SyRI amounts to lawful processing.

As the government and participating institutions have not published documents explaining the purpose of specific SyRI projects, it is not possible to determine whether SyRI complies with the principle of purpose specification and limitation. Although it is clear that the participating institutions have to explicitly specify the purpose of every project, this lack of transparency poses a risk.

According to the data quality principles, data should be relevant and accurate and may only be retained for a limited period of time. Although the participating institutions have to justify the relevancy of the data they intend to use, they have not published information about the data sets they use in specific projects. As SyRI may use a wide range of data sets, it is unclear whether SyRI always complies with this principle. With respect to the accuracy of data, SyRI relies on the data sets provided by the participating institutions. It is not possible to assess whether this data is always accurate. Notwithstanding this lack of transparency, SyRI has several safeguards and procedures in place that would filter out inaccurate data, and only retains data for a limited period of time. Although it is not a specific risk or violation of a principle, it is worrisome that SyRI may use data that was collected for different purposes than fraud detection.

As the government and the participating institutions effectively inform the public of the start and purpose of a SyRI project, there seems to be no clear violation of the principle of fair processing. However, there are a number of risks. As the notifications do not contain information on the identity and address of the involved institutions, it is difficult, if not impossible, for citizens to request additional information. Moreover, there is no possibility for an individual to access his or her personal data.

With respect to the principle of accountability, it is unclear how the Data Protection Authority, as the external oversight body, currently monitors the use of SyRI. Similarly, it is unclear how internal oversight currently takes place.

Therefore, the following is recommended:

- Request information from the government regarding themes and priorities set by the LSI to identify the purpose for the use of SyRI in specific years.
- Request information from the government regarding the approved applications for SyRI projects to identify:
    - specified purposes of approved projects;
    - relevancy of processed data; and
    - accuracy of processed data.
- Request information from the government regarding the rejected applications for SyRI projects to identify:
    - type of projects that are rejected; and
    - grounds for rejection.
- Request information from the government regarding the outcome of approved SyRI projects to identify weak and strong points following from the evaluations.
- Advise the government to notify individual citizens in a more effective and easily accessible manner about the start of intervention team projects.
- Advise the government to inform citizens that institutions may use their personal data, which was collected for a specific purpose, for fraud detection.
- Advise the government to include the address and identity of the relevant data controller when notifying the public of the start of an intervention team project.
- Advise the government to enable data subjects to access their personal data wherever it is processed.
- Advise the government to improve internal oversight to prevent discrimination and stigmatisation following from profiling.
- Advise the government to refer to the existing remedy under the Wbp in the SUWI Act or Decree SUWI.
- Advise the APg to publish information regarding the results of its oversight on the use of SyRI.

Table of Contents

Glossary of Defined Terms

'Controller'	'natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law'[1]
'Personal data'	'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'[2]
'Processing' or 'processing of personal data'	'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'[3]

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive or DPD), Art. 2(d). Available at: <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046>, last accessed 18 March 2016.

[2] DPD, Art. 2(a)

[3] DPD, Art. 2(b)

Glossary of Abbreviations

APg	Data Protection Authority (Dutch: 'Autoriteit Persoonsgegevens', prior to January 2016, 'College Bescherming Persoonsgegegevens', CBP)
CJEU	Court of Justice of the European Union (prior to December 2009, European Court of Justice, ECJ)
CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe)
Decree SUWI	Dutch: 'Besluit Structuur Uitvoeringsorganisatie Werk en Inkomen'
DPD	Data Protection Directive
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
IB	Intelligence Bureau (Dutch: 'Inlichtingenbureau')
LSI	National Steering Committee Intervention Teams (Dutch: 'Landelijke Stuurgroep Interventieteams')
SARI	System Anonymous Risk Indication (Dutch: 'Systeem Anonieme Risico Indicatie')
SVB	Dutch: 'Sociale Verzekeringsbank'
SyRI	System Risk Indication (Dutch: 'Systeem Risico Indicatie')
SUWI Act	Dutch: 'Wet Structuur Uitvoeringsorganisatie Werk en Inkomen'
SZW	Social Affairs and Employment (Dutch: 'Sociale Zaken en Werkgelegenheid')
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

UWV	Dutch: Uitvoeringsorganisatie werknemersverzekeringen’
Wbp	Data Protection Act (Dutch: ‘Wet bescherming persoonsgegevens’)

1. Introduction

Governments employ a wide range of technological devices, systems and programmes to automatically process data. In the Netherlands, one of these programmes is System Risk Indication (SyRI),[4] which can process data sets from different governmental institutions to signal tax and allowance fraud and non-compliance with labour regulations.[5] As SyRI processes personal data, it promotes profiling and has the potential to seriously infringe privacy. Therefore, it should be subject to a number of safeguards.

These safeguards should be based on the law of the Council of Europe (CoE) and European Union (EU), which aim to regulate data processing while limiting privacy infringements. As the Dutch government has not widely publicised SyRI, it remains unclear how and when the system operates.

1.1 Research goals

This memorandum evaluates SyRI in the light of European data protection rules and principles, based on the following research question:

> To what extent does SyRI comply with data protection principles based on Council of Europe and European Union law?

The secondary research question identifies potential risks of non-compliance:

> What are the risks that follow from (partial) non-compliance with data protection principles based on Council of Europe and European Union law?

1.2 Methodology and structure

To answer these research questions, this memorandum contains four parts drawing on both descriptive and evaluative elements. The memorandum starts with an analysis of primary materials to describe SyRI, as there is no comprehensive overview of the system (Section 2). These materials mainly come from the Ministry of Social Affairs and Employment (SZW) and Parliament. This part also serves to rebut the incomplete and often incorrect reports about SyRI in the media. Section 3 outlines the relevant legal framework based on CoE conventions and case law and EU legislation and case law. As these jurisdictions determine the Dutch legal framework, they provide the most appropriate assessment criteria. Section 4 distils the assessment criteria from the legal framework and describes the main elements. Section 5 evaluates SyRI in light of these assessment criteria. Finally, Section 6 and 7 present conclusions and recommendations respectively.

[4] Dutch: 'Systeem Risico Indicatie'.
[5] SUWI Act, Art. 64(1).

2. System Risk Indication

In the Netherlands, governmental institutions use SyRI to detect, prevent and combat fraud. This section first describes the wider context of the fight against fraud in the Netherlands. It then elaborates on the development of data processing systems in this context. The third part explains the procedures and application of SyRI. This section concludes by identifying expected developments.

2.1 Context

In April 2013, Dutch journalists revealed that Bulgarian gangs committed large-scale fraud with social benefits.[6] The gangs brought fellow Bulgarians to the Netherlands, who subsequently registered with the municipality, opened a bank account and applied for allowances. After their applications were approved, they would leave the country and go back to Bulgaria. The gangs then received the payments and paid a small remuneration to the middlemen. This revelation, which occurred after widespread fraud with study grants, led to public outcry.[7]

In response to increased public demand, successive governments have prioritised fraud prevention and detection.[8] Key developments in this respect are the Fraud Act[9] and the Joint Approach to Fraud, both from 2013.[10] The Fraud Act imposes high fines on citizens who provide incomplete or incorrect information when they apply for allowances, even if this is unintentional. According to the National Ombudsman, the Fraud Act is primarily concerned with showing the 'tough, efficient and uniform' stance of the government.[11] The Joint Approach to Fraud aims to harmonise the prevention measures of the national government, with each ministry taking the lead in its own field of expertise.[12] With respect to data sharing, this is the Ministry of Social Affairs and Employment (SZW).[13]

2.2 The path leading to SyRI

The development of data processing systems took place against the background described in Section 2.1. In October 2003, a number of governmental institutions founded the National Steering Committee Intervention Teams (LSI)[14] to coordinate the fight against tax and

[6] KRO Brandpunt (21 April 2013), available at: <http://brandpunt.kro.nl/seizoenen/2013/afleveringen/21-04-2013/fragmenten/gratis-geld-uit-holland/> last accessed 18 March 2016.
[7] e.g. De Volkskrant, '"Studenten frauderen massaal met studiebeurs"' (8 July 2009), available at: http://www.volkskrant.nl/binnenland/-studenten-frauderen-massaal-met-studiebeurs~a339140/ , last accessed 23 April 2016.
[8] *Kamerstukken II* 2014-2015, 32 761, nr. 79, p. 1.
[9] Dutch: 'Fraudewet' (2013), officially: 'Wet aanscherping handhaving en sancties SZW-wetten'.
[10] Dutch: 'Rijksbrede Aanpak Fraude (2013).
[11] Helden, W.J. van, Blaakman, M.J., Catshoek, W.G., Hanse, D.J., Jong-Marsman, C.A. de, Stehouwer, A.,'Geen fraudeur, toch boete: Een onderzoek naar de Fraudewet in de praktijk' (nr. 2014/159, 4 December 2014), p. 1.
[12] *Kamerstukken II* 2014-2015, 17 050, nr. 450, p. 1.
[13] Dutch: 'Ministerie van Sociale Zaken en Werkgelegenheid'.
[14] Dutch: 'Landelijke Stuurgroep Interventieteams'.

allowance fraud and non-compliance with labour regulations.[15] The LSI oversees so-called intervention teams, in which the following institutions may cooperate on specific projects: municipalities, police, the public prosecutor, the Tax and Customs Administration, the Inspection SZW, the Ministries of Finance and SZW and the institutions handling employment benefits (UWV) and other social benefits (SVB).

Since 2006, the Ministry of SZW and intervention teams have experimented with an automated system for fraud detection. Unlike the Fraud Act and the Joint Approach to Fraud, the government has not widely publicised this programme, which initially operated under the name Black Box. According to the Minister of SZW, the development of the system took place in consultation with the Data Protection Authority (APg).[16]

The main task of the APg is to supervise data processing and ensure compliance with applicable law, in particular the Data Protection Act (Wbp).[17] It has the competence to conduct investigations and impose sanctions.[18] In September 2006, the APg published a note on the use of data processing in the fight against fraud setting out the assessment framework it would use in future investigations.[19] The APg stated that an analysis of all individuals within a certain population should take place on the basis of risk models.[20] As these had not been developed yet, the Ministry of SZW and the APg agreed to develop the models within Black Box.[21] The Ministry of SZW also agreed to notify the APg of every relevant project by submitting a list of all types of data used for the project.[22]

In 2007 and 2010, the APg conducted official investigations into Black Box and concluded that some elements were not in compliance with the Wbp.[23] In particular, the APg noted that Black Box had no data security plan, retained data for an unnecessarily long period of time, and did not inform the data subjects of the investigations. In response, the Ministry of SZW changed its methods and appointed the Intelligence Bureau (IB) as the data controller.[24] The IB drafted a data security plan and clear procedures for data retention and notification of subjects. The responsible institutions and the Minister of SZW now notify the affected population in local newspapers[25] and the Government Gazette, respectively.[26]

---

[15] Aanhangsel Handelingen 2014-2015, nr. 429, p. 3.
[16] Aanhangsel Handelingen 2014-2015, nr. 429, p. 3; Dutch: 'Autoriteit Persoonsgegevens'.
[17] Dutch: 'Wet bescherming persoonsgegevens'.
[18] Aanhangsel Handelingen 2014-2015, nr. 429, p. 3.
[19] College Bescherming Persoonsgegevens, 'Notitie fraudebestrijding door bestandskoppeling' (September 2006).
[20] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.
[21] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.
[22] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.
[23] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.
[24] In 2001, the Ministry of Social Affairs and Employment created the Intelligence Bureau (Dutch: 'Inlichtingenbureau') as an independent foundation to support municipalities and other governmental institutions. It serves as the main source of information related to (current) social affairs.
[25] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.
[26] Decree SUWI, Art. 5a.4.1; Dutch: 'Staatscourant'.

Moreover, the Minister of SZW proposed amendments to the existing SUWI Act[27] and SUWI Decree to provide clarity on the use of the system.[28] In these amendments, Black Box was initially renamed System Anonymous Risk Indication (SARI)[29] and eventually System Risk Indication (SyRI).[30] During the legislative process, both the Council of State[31] and the APg expressed their concerns about the extensive implications of the proposed amendments. Both institutions advised the Minister to significantly amend his proposals. Contrary to reports in the media, the Minister considered the recommendations and changed some of the provisions in the amendments.[32] Both Chambers of Parliament passed the final amendments unanimously. According to a spokesperson of the Labour Party, a debate was not necessary as the amendments only clarified existing and accepted practice.[33] Although there was no debate, four parties[34] submitted written questions to the Minister.[35]

2.3 Procedures and application

Articles 64 and 65 of the SUWI Act provide the legal basis for SyRI, while Chapter 5a of the Decree SUWI sets out the rules and procedures. Ultimately, the Minister of SZW is responsible for the use of SyRI.[36]

Each year, on behalf of the Minister of SZW, the LSI determines themes and priorities for investigations.[37] Based on these themes and priorities, participating institutions may start intervention team projects. If an intervention team wants to use SyRI, they have to apply to the Minister of SZW.[38] In their application, the intervention team lists the participating institutions, concrete objective, organisational aspects, intended starting date and duration of the project.[39] Moreover, the intervention team justifies which concrete data, method of risk notification and risk model are applicable.[40] The participating institutions must unanimously agree on the project and check for necessity and proportionality before they share their data.[41] As long as the participating institutions demonstrate the relevance of the data for the purpose

[27] Dutch: 'Wet Structuur Uitvoeringsorganisatie Werk en Inkomen'.
[28] Dutch: 'Besluit SUWI'.
[29] Tomesen, W.B.M., 'Brief aan de Minister van Sociale Zaken en Werkgelegenheid betreffende Advies conceptbesluit SyRI' (ref. z2013-00969, 18 February 2014); Dutch: 'Systeem Anonieme Risico Indicatie'.
[30] *Kamerstukken II* 2012-2013, 33 579, nr. 4.
[31] Dutch: 'Raad van State'.
[32] 'Reactie Minister Asscher op artikel in de Volkskrant over fraudeaanpak' (1 October 2014), available at, https://www.rijksoverheid.nl/actueel/nieuws/2014/10/01/reactie-minister-op-artikel-in-de-volkskrant-over-fraudeaanpak> last accessed18 March 2016.
[33] Information provided by PILP in an email to the authors, dated 23 November 2015.
[34] i.e. PvdA, VVD, SP and CDA
[35] Information provided by PILP in an email to the authors, dated 23 November 2015.
[36] SUWI Act, Art. 65(1).
[37] 'Reactie Minister Asscher op artikel in de Volkskrant over fraudeaanpak' (1 October 2014), available at, https://www.rijksoverheid.nl/actueel/nieuws/2014/10/01/reactie-minister-op-artikel-in-de-volkskrant-over-fraudeaanpak> last accessed18 March 2016.
[38] Decree SUWI, Art. 5a.1.1.
[39] Decree SUWI, Art. 5a.1.2a.
[40] Decree SUWI, Art. 5a.1.2b-d.
[41] Decree SUWI, Art. 5a.1.4.

of the project, they may share almost all types of data on both individuals and legal entities. For example, they may share information about someone's address, education and permits.[42] Following the advice of the Council of State, it is no longer possible to share some sensitive data, such as criminal records.

If the Minister of SZW approves the application, the participating institutions provide the approved data sets to the IB.[43] The IB first pseudonymises the data, then combines the different data sets into profiles and finally compares the profiles to the risk model.[44] These risk models are based on a number of pre-set indicators. The Inspection SZW is responsible for the development of both indicators and risk models on behalf of the Minister.[45] Only if there is a match with the risk model, will the IB decrypt the data and create a risk profile.[46] The IB submits these risk profiles to the Minister for a second analysis[47] and destroys all data within four weeks.[48]

If the second analysis indicates a risk, the Minister submits a risk notification to the appropriate institutions[49] and to the Register Risk Notifications.[50] Based on the notification, the institutions may start proper investigations. Within twenty months after the start of the project, the institutions must provide feedback on the investigations.[51] The Minister uses the feedback to evaluate the risk models.[52] The submission of feedback signals the end of the project.[53] The Minister destroys all data after receipt of the feedback, or within two years after the start of the project at the latest.[54] If the second analysis does not indicate a risk, the Minister must destroy the data within four weeks.[55]

For a two-year period, the Register Risk Notifications may retain all information relevant to the notifications.[56] Data subjects may enquire at the Register Risk Notifications whether they are subject of a notification.[57]

2.4 SyRI in practice

In response to a request by Parliament, the Minister of SZW reported on SyRI in June 2015.[58] This report provides unique insight in the use of the system. Between 2008 and 2014,

[42] Decree SUWI, Art. 5a.1.3.
[43] Decree SUWI, Art. 5a.2.1.
[44] Decree SUWI, Art. 5a.2.3.
[45] Decree SUWI, Art. 5a.1.7.
[46] Decree SUWI, Art. 5a.2.3f.
[47] Decree SUWI, Art. 5a.2.3g.
[48] Decree SUWI, Art. 5a.2.4.
[49] Decree SUWI, Art. 5a.3.2.
[50] Decree SUWI, Art. 5a.5.1; Dutch: 'Register Risicomeldingen'.
[51] Decree SUWI, Art. 5a.3.4.
[52] Decree SUWI, Art. 5a.6.
[53] Decree SUWI, Art. 5a.4.2.
[54] Decree SUWI, Art. 5a.3.5.
[55] Decree SUWI, Art. 5a.3.3.
[56] Decree SUWI, Art. 5a.5.5.
[57] Decree SUWI, Art. 5a.5.3.
[58] *Kamerstukken II* 2014-2015, 17 050, nr. 508, p. 1.

intervention teams started 160 projects. In 22 of these projects, the respective intervention teams used SyRI. As one of these 22 projects had not been completed, the Minister did not include it in his report.[59] Out of the other projects, 19 focused on specific neighbourhoods, one on a recreational area and one specifically on asset fraud by individuals with an allowance based on the Labour and Social Assistance Act.[60] With these projects, the government collected €20.5 million worth of fines and adjusted taxes and allowances.[61]

2.5 Expected developments

The Dutch government is currently drafting new legislation to facilitate data sharing between governmental institutions and possibly private parties.[62] At the moment, the relevant legislation differs per sector. Therefore, the government advocates a 'broad and integral approach' to improve cooperation between institutions.[63] In December 2013, the Cabinet announced that it had appointed a working group to explore the possibility and desirability of a Data Sharing Act.[64] In their report, which the Minister of Security and Justice[65] sent to Parliament in December 2014, the working group advised the government to start the drafting process.

In February 2015, the APg published a preliminary opinion on the new law.[66] The APg identified two basic problems. Firstly, it argued that, rather than developing new legislation, the government should optimise existing legislation. Secondly, it argued that the proposed law would not allow for testing specific projects against the principles of necessity, proportionality, subsidiarity and foreseeability, as it is simply too broad to meet these requirements of the Wbp.[67] Since the reaction of the APg, neither the government nor the APg have publicised new developments.[68] Efforts to reach out to the APg and the Ministry of SZW have not resulted in additional information about the current status of the Data Sharing Act.

[59] *Kamerstukken II* 2014-2015, 17 050, nr. 508, p. 1.
[60] Dutch: 'vermogensfraude gepleegd door personen met een uitkering op grond van de Wet werk en bijstand'.
[61] *Kamerstukken II* 2014-2015, 17 050, nr. 508, p. 1.
[62] 'Kennis delen geeft kracht: Naar een betere èn zorgvuldigere gegevensuitwisseling in samenwerkingsverbanden', attached to: *Kamerstukken II* 2014-2015, 32 761, nr. 79, p. 5.
[63] *Kamerstukken II* 2014-2015, 32 761, nr. 79, p. 1; Dutch: 'brede en integrale benadering'.
[64] Dutch: 'Kaderwet Gegevensuitwisseling'.
[65] Dutch: 'Minister van Veiligheid en Justitie'.
[66] Tomesen, W.B.M. 'Brief aan de Minister van Veiligheid en Justitie betreffende Verkenning kaderwet gegevensuitwisseling' (25 February 2015).
[67] Dutch: 'Wet Bescherming Persoonsgegevens'.
[68] Autoriteit Persoonsgegevens, available at: <http://www.autoriteitpersoonsgegevens.nl> last accessed 18 March 2016; Rijksoverheid, available at: <http://www.rijksoverheid.nl> last accessed 18 March 2016.

3. Legal framework

The CoE and EU determine the Dutch legal framework regarding data protection and data processing. This section outlines the relevant legal provisions that provide the basis for the assessment framework in Section 4, which will be applied to SyRI in Section 5.

3.1 Council of Europe

A number of legal sources coming from the CoE are binding upon the Netherlands. In the context of data protection and processing, the most important sources are:

i. the European Convention on Human Rights (ECHR), including the original Convention for the Protection of Human Rights and Fundamental Freedoms and the amending Protocols;
ii. the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108); and
iii. case law from the European Court of Human Rights (ECtHR).

The below sub-sections will go into greater detail concerning the legal framework.

3.1.1 ECHR

As SyRI is an automatic data processing programme that could infringe the right to privacy, its assessment primarily depends on Article 8 of the ECHR, which stipulates:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

3.1.2 Convention 108

The purpose of this Convention is to secure for individuals in the territory of each Member State respect for their fundamental rights and freedoms, particularly related to the right to privacy, protection of personal data and regulation of automatic processing of personal data. The Convention contains several provisions about the duties of data controllers and the rights of data subjects. These include but are not limited to:

> Article 5 – Quality of data
>
> Personal data undergoing automatic processing shall be:
>
> a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 8 – Additional safeguards for the data subject

Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;
d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

3.1.3 Case law

In the context of data protection and data processing, the following case law of the ECtHR is of key value:

- ECtHR (1979), *Sunday Times v. United Kingdom*
- ECtHR (1983), *Silver and Others v. United Kingdom*
- ECtHR (1987), *Leander v. Sweden*
- ECtHR (1999), *Kopp v. Switzerland*
- ECtHR GC (2000), *Amann v. Switzerland*
- ECtHR GC (2009), *S and Marper v. UK*
- ECtHR (2009), *Haralambie v. Romania*
- ECtHR (2009), *K.H. and Others v. Slovakia*
- ECtHR (2010), *Kennedy v. UK*
- ECtHR (2012), *Iordachi v. Moldova*

These cases return throughout Sections 4 and 5 of the memorandum. Its relevant implications are explained in the context of the principles discussed in those sections.

3.2 European Union

A number of legal sources coming from the EU are directly binding upon the Netherlands.[69] In the context of data protection and processing, the most important sources are:

i. the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU);
ii. the Charter of Fundamental Rights of the European Union (EU Charter);
iii. EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive or DPD);[70] and
iv. case law of the Court of Justice of the European Union (CJEU).

The following sub-sections discuss these sources in greater detail.

3.2.1 TEU and TFEU

The TEU outlines general interests and aims that the EU seeks to uphold and achieve, such as peace, stability and economic cooperation. The TFEU contains Article 16 as a relevant element to data protection, putting forward:

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

3.2.2 Articles 7 and 8 of the EU Charter

The EU Charter contains the following articles relevant to the area of data protection and data processing:

> Article 7
>
> Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8

[69] Case 26/62 *Van Gend en Loos* [1963] ECR 1.
[70] EU Directive 95/46/EC, available at: <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046> last accessed 18 March 2016.

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

3.2.3 Data Protection Directive 95/46/EC

The DPD contains rules for the entire range of data protection and data processing. Relevant provisions include but are not limited to:

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) 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 or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

3.2.4 Case law

The CJEU interprets EU law and has also interpreted key EU law in the context of data protection and data processing. In its landmark *Digital Rights Ireland* case, the CJEU held that the EU legislature had exceeded the limits of the proportionality principle in relation to Articles 7 and 8 of the EU Charter by adopting the Data Retention Directive, through which Member States could deviate from the principles laid down in the DPD.[71]

[71] Cases C-293/12 and 594/12 *Digital Rights Ireland* [2014] 3 W.L.R. 1607.

4. Assessment framework

Based on the legal framework in the preceding section, this section develops an assessment framework for data processing through SyRI. The assessment framework contains the following five principles derived from the CoE and EU jurisdictions: the principles of lawful processing; purpose specification and limitation; data quality; fair processing; and accountability.

4.1 Principle of lawful processing

According to CoE and EU law, processing personal data has to be lawful.[72] However, neither body of law has codified 'lawful processing'. The parameters of what processing is lawful are therefore determined by using the notion of *justified interference* as found in ECtHR jurisprudence and the conditions for *lawful limitations* as found in Article 52 of the EU Charter.

4.1.1 CoE: justified interference

Under the CoE regime, the processing of personal data may constitute an interference with the right to respect for private and family life.[73] If processing of personal data does amount to an interference, such an interference must be justified. Interferences are justified if they are:

i. in accordance with the law;
ii. pursuing a legitimate aim; and
iii. necessary in a democratic society.[74]

An interference is in accordance with the law if it has a basis in domestic law. This law must be accessible, the effects of the law must be foreseeable and the use of the law must be compatible with the rule of law.[75] A law is accessible if it is publicly available. Its effects are foreseeable if the formulation is precise enough for an individual to regulate his or her conduct accordingly.[76] This does not imply that an individual has to be able to foresee an interference,[77] but clear and detailed rules must specify the conditions of a legitimate interference. The use of a law is compatible with the rule of law if it prevents arbitrary interferences with an individual's rights. Sufficient and adequate safeguards, such as (independent) oversight and effective remedies, should thus protect an individual against abuse. Moreover, an individual should receive a notification or have the possibility to obtain knowledge in case of an interference with his or her rights.[78]

---

[72] Convention 108, Art. 5(a); DPD, Art. 6(1(a)).
[73] ECHR, Art. 8.
[74] ECHR, Art. 8(2).
[75] *Kopp v. Switzerland* App No. 23224/94 [1999] 27 E.H.R.R. 91 [55]; *Amann v. Switzerland* App No. 27798/95 [2000] 30 E.H.R.R. 843 [50].
[76] *Sunday Times v. United Kingdom* App No. 6538/74 [1979-80] 2 E.H.R.R. 245 [49]; ECtHR, *Silver and Others v. United Kingdom*, App Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 [1983] 5 E.H.R.R. 347 [88]; *Amann v. Switzerland* App No. 27798/95 [2000] 30 E.H.R.R. 843 [56].
[77] *Iordachi v. Moldova* App No. 25198/02 [2012] 54 E.H.R.R. 5 [39].
[78] These safeguards can, amongst others, be found in *Kennedy v. UK* App No. 26839/05 [2010] 52 E.H.R.R. 4.

An interference must pursue a legitimate aim, such as: 'the interests of national security, public safety or the economic wellbeing of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others'.[79]

An interference is justified if it is necessary in a democratic society, meaning that it coincides with a pressing social need. In addition, the interference must be proportionate to the legitimate aim pursued.[80]

4.1.2 EU: lawful limitations

Under the EU regime, Article 52(1) of the EU Charter contains the conditions for lawful limitations on the exercise of the rights and freedoms recognised in the Charter. These conditions have to comply with the conditions for a justified interference under the ECHR.[81] The EU regime can, however, provide for more protection than the ECHR.[82]

The conditions for a lawful limitation are that:

i. the law provides for the limitation;
ii. the limitation respects the essence of the rights and freedoms recognised by the Charter;
iii. the limitation is necessary, subject to the principle of proportionality; and
iv. the limitation genuinely meets objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Processing of personal data can limit the rights under Articles 7 and 8 of the EU Charter. Pursuant to Article 7 of the EU Charter, data processing can limit the right to respect for private and family life. The meaning and scope of Article 7 of the EU Charter are the same as those of Article 8 of the ECHR.[83] Therefore, a limitation on Article 7 of the EU Charter is only lawful if an interference is justified under Article 8 of the ECHR.[84]

Data processing can limit the right to protection of personal data, as found in Article 8 of the EU Charter. The limitation must meet both the requirement of a justified interference in accordance with the CoE framework and the conditions for lawful limitations as put forward by the EU framework. Article 8 of the EU Charter has its basis in the DPD. This Directive contains conditions and limitations for the exercise of the right to the protection of personal data.[85] If data processing respects all data protection principles in Section 4, it also respects the right to protection of personal data. According to the CJEU, the essence of the right to

[79] ECHR, Art. 8(2).
[80] *Leander v. Sweden* App No. 9248/81 [1987] 9 E.H.R.R [58].
[81] EU Charter, Art. 52(3); TEU, Art. 6(3).
[82] EU Charter, Art. 52(3), last sentence.
[83] In accordance with EU Charter, Art. 52(3).
[84] EU Charter, Art. 52(3); Explanations relating to the Charter of Fundamental Rights, (2007/C 303/02), Official Journal of the European Union C 303/17, Title II, explanation on Article 7.
[85] Explanations relating to the Charter of Fundamental Rights, (2007/C 303/02), Official Journal of the European Union C 303/17, Title II, explanation on Article 8.

data protection is to ensure that 'appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data'.[86]

The EU and the CoE regimes use the above criteria to determine whether data processing justifies an interference with a right or lawfully limits the enjoyment of a right. Taken together, this may amount to *lawful processing*.

4.2 Principle of purpose specification and limitation

The legitimacy of processing personal data depends on the purpose of the processing and on whether that purpose has been clearly and sufficiently conveyed before the processing starts.[87] The processing of personal data for undefined or unlimited purposes is unlawful.

Under CoE law, Article 5(b) of Convention 108 requires personal data to be 'stored for specified and legitimate purposes and not used in a way incompatible with those purposes'. EU law further defines this principle in Article 6(1)(b) of the DPD, which requires that personal data must be processed:

i. for a specified purpose;
ii. for an explicit purpose;
iii. for a legitimate purpose; and
iv. not in a manner incompatible with the original purpose.

Article 6(1)(b) of the DPD requires the specific identification of the purpose of the processing. The purpose must be detailed enough to determine the kind of processing used, and to allow for an assessment of compliance with the law and the application of safeguards.[88]

Article 6(1)(b) of the DPD requires a clear and intelligible presentation of the purpose of the processing, preventing vagueness or ambiguity as to the meaning or intent of the purpose. The requirement for an explicit purpose differs from the requirement to provide information to the data subject (Articles 10 and 11 of the Directive) and the requirement to notify the supervisory authority (Article 18). Nevertheless, all three requirements are closely related and they all serve the ultimate purpose of transparency.[89] Section 4.4 on the principle of fair processing elaborates on this.

Article 6(1)(b) of the DPD requires the purpose of the processing to be 'in accordance with the law' in the broadest sense. This includes all forms of law: primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence.[90]

[86] Cases C-293/12 and 594/12 *Digital Rights Ireland* [2014] 3 W.L.R. 1607 [40].
[87] Under the CoE regime, this is regulated by Convention 108, Art. 5(b); under the EU regime, this is regulated by the Data Protection Directive, Art. 6(1)(b).
[88] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203, Brussels, 2 April 2013) p. 15.
[89] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203, Brussels, 2 April 2013) p. 17.
[90] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203, Brussels, 2 April 2013) p. 19.

Article 6(1)(b) of the Directive provides that personal data collected for one or more purposes shall 'not be further processed in a way incompatible with those purposes'. This means that further use of data for another purpose needs an additional legal basis if the new purpose of processing is incompatible with the original purpose. A new purpose requiring such an additional legal basis includes the transfer of data to third parties.

4.3 Data quality principles

Once the controller explicitly specifies a legitimate purpose, the data quality principles have to be met. Following this principle, data must be:

i. relevant;
ii. accurate; and
iii. retained for a limited period of time.

According to the DPD and Convention 108 processing can only occur if it is 'adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed'.[91] Therefore, there must be a purpose clearly defined for the data for an assessment of relevancy to be made.

Article 6(1) (d) of the DPD and Article 5(d) of Convention 108 covers accuracy. Both require data to be accurate and kept up to date. The DPD goes further to require reasonable steps are taken to either erase or rectify data which is inaccurate or incomplete. Accuracy is paramount due to the fact that damage could be caused if inaccurate data is used, such as in the allocation of social welfare.

Pursuant to Article 6(1)(e) of the DPD and 5(e) of Convention 108, retention of data covers the period of time for which the controller of the data is permitted to hold the data. The aforementioned provisions require data be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.' Therefore, data may no longer be retained once the purposes have been served. For the CoE, *S and Marper*[92] requires data retention to be proportionate for the aforementioned relevant purposes.[93]

Furthermore, in the *Digital Rights Ireland* case, the CJEU recognised that the EU Charter is relevant with regard to the validity of law regulating data processing, which was in that case the Data Retention Directive.[94] It then moves on to say that this Directive deviates from the normal data protection regime. The interferences by the Directive with the rights enshrined in the Charter could be justified if they meet all relevant requirements, but the CJEU held that the proportionality requirement was not met. The Directive provided too few safeguards for

[91] Convention 108, Art 5(c); DPD, Art 6(1)(c).
[92] *S. and Marper v. United Kingdom* App Nos. 30562/04 and 30566/04 [2009] 48 E.H.R.R. 50.
[93] *S. and Marper v. United Kingdom* App Nos. 30562/04 and 30566/04 [2009] 48 E.H.R.R. 50 [107].
[94] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>, last accessed 18 March 2016.

the limits, use and protection of the data retained.[95] This means the EU legal framework prescribes a strong proportionality assessment in cases of infringements with Charter rights.

4.4 Principle of fair processing

The principle of fair processing regulates the relationship between the data controller and the data subject. The controller has an obligation to inform data subjects about the use of their data and also to keep the data subjects informed. Five criteria apply to this obligation to inform:

i. the controller must provide the information in an effective[96] and easily accessible way. In addition, if a data subject asks whether the data controller uses his or her data for data processing, the controller must provide this information;
ii. the information should at least address the purpose of the processing and the identity and address of the controller;
iii. data subjects have the right to access their data wherever the controller processes this data;[97]
iv. unless the law specifically provides for it, a controller is not allowed to secretly process personal data; and
v. third parties may only have limited access to personal data. In the *Digital Rights Ireland* case the CJEU stated that the Data Retention Directive did not sufficiently limit access to data and thus declared it invalid. Other parties should only have access to personal data for the prevention, detection or prosecution of offences sufficiently serious to warrant interference with fundamental rights.[98]

4.5 Principle of accountability

The preceding paragraphs show four principles that data controllers have to comply with when processing personal data. Article 6(2) of the DPD states that the controller is responsible for compliance with the principles related to lawful processing, purpose specification and limitation, data quality and fair processing. Although CoE and EU law do not provide clarity regarding the content of the principle of accountability, it is clear that a controller must comply with data protection rules and principles, and that the responsibility lies with the controller. This implies two things:

i. the determination of compliance requires oversight; and
ii. non-compliance requires a remedy.

Article 28(1) of the DPD requires every EU Member State to establish one or more independent public authorities responsible for monitoring the application of the provisions adopted by the Member States pursuant to the DPD. Such an authority must have several powers to be able to exercise its supervisory duties. These powers include but are not limited

[95] Cases C-293/12 and 594/12 *Digital Rights Ireland* [2014] 3 W.L.R. 1607 [60], para. 65ff.
[96] *Haralambie v. Romania* App No. 21737/03 27 October 2009.
[97] *K.H. and Others v. Slovakia* App No. 32881/04 28 April 2009.
[98] Cases C-293/12 and 594/12 *Digital Rights Ireland* [2014] 3 W.L.R. 1607 [60].

to the power to access data forming the subject matter of processing operations and the power to intervene by imposing a ban on processing.[99]

Article 22 of the DPD requires Member States to provide for judicial remedies for any breach of rights of individuals, following from processing of their personal data. If an individual suffers damage as a result of such a breach, the controller must provide compensation to that individual.[100] This rule does not apply if the controller proves that he or she is not responsible for the event giving rise to the damage.[101] Convention 108 contains a similar provision.[102]

[99] DPD, Art. 28(3).
[100] DPD, Art. 23(1).
[101] DPD, Art. 23(2).
[102] Convention 108, Art. 10.

5. Assessment of SyRI

5.1 Principle of lawful processing

SyRI processes personal data by combining data sets from different governmental institutions in the fight against fraud. The processing of personal data in SyRI constitutes an interference with the right to privacy under Article 8 of the ECHR and a limitation of the rights under Articles 7 and 8 of the EU Charter. The following section determines whether the use of SyRI constitutes a justified interference and a lawful limitation, and, therefore, assesses if its use amounts to lawful processing. Section 5.1.1 first assesses the interference with Article 8 of the ECHR and the limitation of the right in Article 7 of the EU Charter to determine whether the interference is justified and the limitation is lawful. Section 5.1.2 then assesses whether the limitation of the enjoyment of the right under Article 8 of the EU Charter is lawful. Section 5.1.3 finally identifies possible risks related to the principle of lawful processing.

5.1.1 Lawful processing: right to respect for private and family life

Processing of personal data in SyRI interferes with the right under Article 8 of the ECHR and limits the enjoyment of the right under Article 7 of the EU Charter, which both contain the right to respect for private and family life. This section analyses whether the interference is in accordance with the law, pursues a legitimate aim and is necessary in a democratic society. If an interference with Article 8 of the ECHR is justified, a limitation of the enjoyment of the right under Article 7 of the EU Charter is also lawful.

The use of SyRI has a basis in Dutch law in Articles 64 and 65 of the SUWI Act and Chapter 5a of the Decree SUWI. Since both the SUWI Act and the SUWI Decree are published online they are publicly accessible. As the law clearly describes what individuals should and should not do, the effects of the law are foreseeable. The purpose and procedures as laid down in the SUWI Act and the Decree SUWI prevent arbitrary use of the system and ensure respect for the rule of law.

Additionally, the use of SyRI pursues a legitimate aim, because Article 64(1) of the SUWI Act states that the system is used for the prevention and combatting of several forms of fraud. Therefore, the system is used for the 'prevention of crime' and to ensure the 'economic wellbeing' of the Netherlands.[103] So far SyRI projects have resulted in the collection of €20.5 million worth of fines and adjusted taxes and allowances.[104]

As the use of SyRI coincides with a pressing social need, it is necessary in a democratic society. This need is the increased public demand to prioritise fraud prevention and detection.[105] Before a project can start, the intervention team has to specifically request the use of data necessary to achieve the specified purpose. The intervention team may only use the data that is necessary and relevant for that specified purpose. If personal data does not

[103] See ECHR, Art. 8(2).
[104] *Kamerstukken II* 2014-2015, 17 050, nr. 508, p. 1.
[105] *Kamerstukken II* 2014-2015, 32 761, nr. 79, p. 1.

qualify as such, the data controllers will not use it for the analysis and risk notification.[106] By following this procedure and by only allowing the use of relevant data, the use of SyRI seems to be proportionate.

Based on this analysis, it seems that the interference with the right under Article 8 of the ECHR is justified and the limitation of the enjoyment of the right under Article 7 of the EU Charter is lawful. Therefore, processing of data in SyRI does not violate the principle of lawful processing in relation to the right to respect for private and family life.

5.1.2 Lawful processing: right to protection of personal data

Processing personal data in SyRI also limits the enjoyment of the right under Article 8 of the EU Charter, which contains the right to protection of personal data. This provision does not have a verbatim corresponding right in the ECHR, but is partly based on Article 8 of the ECHR.[107] This section analyses whether the limitation is a justified interference and whether the limitation has a legal basis, respects the essence of the rights and freedoms recognised by the Charter, is necessary and genuinely meets objectives of general interest recognised by the Union or the need to protect the right and freedoms of others.

As the previous section shows, the use of SyRI has a legal basis, pursues a legitimate aim and is necessary and proportionate. SyRI thus meets the conditions for a justified interference with regard to Article 8 of the ECHR and the legal basis and necessity requirements under the EU framework as well.

The use of SyRI also ensures the essence of the right to data protection. The detailed outline of the mandatory procedure for the use of SyRI ensures the use of appropriate technical and organisational measures to prevent accidental or unlawful destruction, accidental loss or alteration of the data. Sections 5.3, 5.4 and 5.5 on the principles of data quality, fair processing and accountability further elaborate on this.

Chapter 6 of the TFEU describes its general interest to encompass the combatting of fraud. Therefore, the use of SyRI to detect, prevent and combat fraud meets this objective.

Based on this analysis, it seems that the limitation of the enjoyment of the right under Article 8 of the EU Charter is lawful. Therefore, processing of data in SyRI does not violate the principle of lawful processing in relation to the right to the protection of personal data.

5.1.3 Risks

Although the use of SyRI constitutes an interference with the right to respect for private and family life and a limitation of the enjoyment of this same right and of the right to protection of personal data, it seems that this interference is justified and that the limitation is lawful. This leads to the conclusion that the use of SyRI amounts to lawful processing, as long as the safeguards remain in place. There are no apparent risks regarding the principle of lawful

[106] Decree SUWI, Art. 5a.1.4b, d.

[107] EU Charter, Art. 52(3); Explanations relating to the Charter of Fundamental Rights, (2007/C 303/02), Official Journal of the European Union C 303/17, Title II, explanation on Article 8.

processing, though there may be issues with redress if the data controller does not comply with the conditions for lawful processing. Additionally, there is a looming potential threat of stigmatisation due to profiling, which in turn could lead to discrimination. This stigmatisation could, amongst other examples, take place when specific social groups are targeted by SyRI projects or when SyRI projects concentrate on neighbourhoods with many immigrants. Section 5.5 elaborates on these matters.

5.2 Principle of purpose specification and limitation

The second principle for legitimate data processing requires a clearly defined and limited purpose. The following section assesses whether data processing in SyRI has a specified, explicit and legitimate purpose, and whether any further processing of data is not incompatible with the original purpose.

The Ministry of SZW developed SyRI to combat tax and allowance fraud and non-compliance with labour regulations.[108] Within this general purpose, the LSI each year determines more specific themes and priorities. Based on these themes and priorities, participating institutions can form intervention teams and request permission from the Minister to start intervention team projects. In its application, an intervention team has to justify the project and identify the 'concrete aim of the cooperation'.[109] Moreover, it has to describe the characteristics of the project and justify the use of the data sets, indicators and risk models.[110] The application most likely contains sufficient detail to determine the specific purpose of a project.[111] However, as the government and participating institutions have not publicised specific applications, it is not possible to assess the purpose of specific projects.

As all intervention team projects must fall within the general purpose of SyRI, as laid down in Articles 64 and 65 of the SUWI Act, they generally serve a legitimate purpose. This legitimate purpose is mainly to combat forms of social security fraud and it consequently seeks to meet interests of public demand, crime prevention and economic wellbeing.

Since all data processing in SyRI takes place to achieve a specific purpose, there is little risk for incompatibility with the purpose of SyRI. However, SyRI uses and combines existing data sets. Citizens have provided these data sets over the course of separate and unrelated interactions with governmental organs pursuing a variety of purposes. These include but are not limited to: applying for permits with municipalities, applying for benefits with the competent authority and filing income tax statements with the Tax and Customs Administration. Using data which citizens have submitted for a specific purpose for a subsequent *new* purpose, requires a separate legal basis. As SyRI provides an additional legal basis for further processing of data, this condition seems fulfilled from a formalistic point of view. Yet, it remains questionable if this additional legal basis would pass the proportionality assessment. After all, although the legislation has been publicised through the official

[108] SUWI Act, Arts. 64(1) and 65(1).
[109] Decree SUWI, Art. 5a.1.2a; Dutch: 'concrete doelstelling van de samenwerking'.
[110] Decree SUWI, Art. 5a. 1.2.
[111] Decree SUWI, Art. 5a.1.2.

channels, citizens have not been notified directly and adequately about this new use of their data, let alone that they explicitly consented to the use of their data for such new purposes, which could make the processing disproportionate.

A potential risk in relation to the principle of purpose specification and limitation is the lack of transparency. As the government and participating institutions have not publicised specific applications of SyRI, it is not possible to assess the purpose of specific projects or the reasonableness and proportionality of a request. However, it seems that the Decree SUWI provides sufficient safeguards against abuse, since Articles 5a.1.4c and 5a.1.4e require the intervention team to conduct a proportionality assessment and to justify the use of SyRI as the least intrusive manner to reach the specified purpose. The Minister is ultimately responsible for this proportionality assessment.

5.3 Data quality principles

The third principle for legitimate data processing requires the use of relevant and accurate data. Moreover, the controller may only retain the data for a limited period of time.

A data controller may only use data that is relevant to a specific purpose. Within the framework of SyRI, an intervention team must justify which 'concrete data' it intends to use at the start of the investigation.[112] Therefore, SyRI may only process the data necessary to combat fraud in order to qualify as adequate, relevant and not excessive in relation to the purpose for which the data is collected and/or further processed. It is unclear whether intervention teams have used data that would not qualify as such. Situations in which irrelevant data is used without a justification are conceivable, which is why redress and accountability are so important. Section 5.5 elaborates on this matter.

Additionally, a controller must take reasonable steps to either erase or rectify inaccurate or incomplete data. The Decree SUWI does not provide any guidance on this principle. As SyRI is not a database, but rather a tool for combining data sets, it depends on the participating institutions for accurate and complete data. Since analysis takes place in three different stages, data controllers can filter out inaccurate and incomplete at separate occasions. Moreover, as any sanction will depend on further investigation by the competent institution, the analysis of SyRI is not conclusive, as such diminishing the risk data posed by inaccurate and incomplete data.

A data controller may only retain data for as long as it necessary and proportionate in relation to the purpose. Within the framework of SyRI, the Decree SUWI provides safeguards for data retention. After the first analysis, the IB destroys all data within four weeks.[113] Similarly, the Inspection SZW destroys all data not leading to risk notifications within four weeks[114] and the remaining risk notifications are destroyed within two years after the start of a project.[115] The Minister is responsible for the Register Risk Notifications and destroys the notification within

[112] Decree SUWI, Art. 5a.1.2b.
[113] Decree SUWI, Art. 5a.2.4.
[114] Decree SUWI, Art. 5a.3.3.
[115] Decree SUWI, Art. 5a.4.5.

two years after registration.[116] These lengths of time appear reasonable. Most of the data is destroyed within four weeks and only those risk notifications which could potentially lead to further investigation are retained for two years. This destruction only regards the notification itself, not the underlying data. Although the CJEU has held that retaining data with a maximum of two years without providing objective and sufficient safeguards is excessive,[117] the way data is handled with respect to SyRI seems reasonable as most data is destroyed within four weeks and only remaining risk notifications are retained for two years. As these risk notifications are merely notifications, they do not contain personal data.

Since SyRI depends on the data requested by the intervention team, it is conceivable that it uses irrelevant or inaccurate data. An intervention team may intentionally or unintentionally request this data. The intention is relevant to the proportionality assessment. Especially when considering that inaccurate or irrelevant data may also be used as a consequence of prejudice or generalisations. This inaccurate or irrelevant data might then lead to wrongful profiling and consequently to stigmatisation and discrimination. This also highlights the importance of internal and external oversight.

5.4 Principle of fair processing

The fourth principle mainly entails that data processing must take place in a transparent manner. The involved institutions should provide information regarding the use of SyRI in an effective and easily accessible way. This information should at least address the purpose of the processing and the identity and address of the controller. Data subjects also have the right to access their data wherever their data is processed. Moreover, controllers cannot process data in secret and third parties cannot have access to the personal data.

Section 2.3 makes clear that intervention teams can start a project to detect and/or prevent a certain form of fraud. An intervention team may use SyRI to support such a project. At the start of a project, the Minister notifies the public in the Government Gazette.[118] The participating institutions also notify a specific area through publication in local newspapers.[119] This is how data subjects can know that an intervention team may process their personal data for the purposes of the project. This seems an effective and easily accessible method of providing information, although it requires individuals to actively access and read these sources. According to the Minister, it would require a disproportionate effort to notify individual citizens. Arguably, the current state of technology enables the government to notify individual citizens in a more effective and easy manner.

The notification of the public at the start of a project contains the purpose of the investigation and the specific area. An example of an intervention team project is the investigation into ‘address fraud’ in the ‘Afrikaanderwijk’ in Rotterdam, which started on 1 February 2016.[120] It

[116] Decree SUWI, Art. 5a.5.5; Dutch: ‘Register risicomeldingen’.
[117] Cases C-293/12 and 594/12 *Digital Rights Ireland* [2014] 3 W.L.R. 1607 [60], para. 63-65.
[118] Decree SUWI, Art. 5a.1.1.
[119] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.
[120] Mededeling van de Minister van Sociale Zaken en Werkgelegenheid van 21 januari 2016, 2016-0000008242, betreffende de aanvangsdatum van het SyRI-project Adresfraude Afrikaanderwijk te Rotterdam, *Staatscourant*

is not clear whether SyRI has been used in this project.[121] An intervention team will not identify the purpose of the investigation in more detail than 'preventing and detecting address fraud', since this could give away the methods of investigation and provide citizens with an opportunity to manipulate the system.[122] A notification does not contain the address and identity of the controller. Article 64 (1(a-d)) of the SUWI Act does show the institutions that can use SyRI for the detection of fraud. The notifications in the Government Gazette do not, however, make clear which specific institutions work together for a particular project. An individual will therefore not know which specific institution to contact for information about the processing of his or her data. Individuals, when initially submitting their personal data, may also not know which institutions ultimately process their data through SyRI.

Pursuant to Article 5a.5.1 of the Decree SUWI, data subjects have the right to enquire whether they are subject of a risk notification. They can only receive a confirmation if they are in the Register Risk Notifications and have no access to the processed data. It appears that data subjects who are not subject of a risk notification have no access at all. Therefore, SyRI does not provide for an individual to access personal data wherever it is processed.

In theory, controllers cannot process personal data in secret. Article 65(2) of the SUWI Act clearly states that a controller can only process personal data for the specified purpose. Whether controllers process data in secret cannot be determined in practice. The obligation for the institutions to follow a specific procedure, before the system can be used for processing, does however seem to ensure that controllers only process personal data for the determined purpose and not for other secret purposes.

Since an intervention team must directly request the use of SyRI, only the appropriate institutions within the team will receive a risk notification from the Minister, if an analysis leads to such a notification.[123] Only if the team wants to use the risk notification for further investigation into a specific individual or individuals, it may retain the notification for two years.[124] If the analysis does not lead to further investigation, the Minister destructs the risk notification after four weeks.[125] It is important to note that this notification does not contain personal data. It is a file containing a risk notification, which indicates the possibility that a certain person or certain persons may be committing a specific form of fraud. The controller deletes all the documents, which contain personal data and which are used for the risk notification, after four weeks.[126] Moreover, everyone involved in the whole process of a risk notification by SyRI must respect a legal obligation of confidentiality.[127]

---

nr. 3826, 29 January 2016, available at: <https://zoek.officielebekendmakingen.nl/stcrt-2016-3826.html> last accessed 18 March 2016.

[121] This again showcases the lack of transparency of SyRI-related projects.

[122] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.

[123] Decree SUWI, Art. 5a.3.2.

[124] SUWI Act, Art. 65(6).

[125] Decree SUWI, Art. 5a.3.3

[126] Decree SUWI, Art. 5a.2.4.

[127] SUWI Act, Art. 65(4).

The relevant institutions must use SyRI in accordance with the principle of fair processing. SyRI complies with some of the elements inherent to the principle of fair processing. Firstly, by notifying the public of an investigation in the Government Gazette and local papers, individuals have relatively effective and easy access to this information. Secondly, such a notification states the purpose in a general manner, without giving away the methods of investigation and without providing citizens with an opportunity to manipulate the system. Thirdly, controllers cannot secretly process data in SyRI, since a controller may only use data in one specific procedure and for one specific purpose. Fourthly, it seems that third parties do not have access to the personal data that are used for the creation of a risk analysis. It is unclear what the consequences are if a data controller fails to comply with these principles.

However, the institutions do not use SyRI in accordance with all elements of the principle of fair processing. Firstly, notifications do not provide information on the identity and address of the involved institutions. This makes it very difficult for an individual to determine which institution to contact for specific information regarding the processing of his or her personal data. Secondly, if an individual succeeds in finding out which institution processes his or her data, no possibility exists to access the personal data wherever the institution processes this data. An individual will therefore only know that an institution uses his or her data for processing, but not which data the institution uses for this purpose. An individual can therefore not object to the use of specific data.

5.5 Principle of accountability

When a data controller uses an automated system for the processing of personal data, the data controller is responsible for complying with the principles of lawful processing, purpose specification and limitation, data quality and fair processing. An independent public authority must keep external oversight and monitor whether the controller complies with those principles. In addition it is recommendable to also have an effective internal oversight mechanism. If a controller does not comply with one of the principles, a data subject must have access to a judicial remedy. The following section assesses whether one or more independent public authorities monitor the conduct of the controllers that use SyRI for processing of personal data and whether data subjects have access to remedies if controllers violate their rights.

An independent public authority must keep external oversight and monitor the conduct of a controller when he or she processes personal data. In the Netherlands, the APg is the competent authority monitoring data processing.[128] In theory, the APg should also monitor the use of SyRI, since data controllers using SyRI process personal data. The APg does seem involved in matters regarding SyRI. According to the Minister of SZW, the development of Black Box, which preceded SyRI, took place in consultation with the APg.[129] In addition, the APg seems to have contributed to the development of the risk models, which were used by controllers in Black Box.[130] Moreover, SZW agreed to notify the APg of every relevant

[128] Wbp, Arts. 51 and 52(2).
[129] Aanhangsel Handelingen 2014-2015, nr. 429, p. 3.
[130] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.

project by submitting a list of all types of data used for that project.[131] In 2007 and 2010, the APg conducted official investigations into Black Box and concluded that some elements were not in compliance with the Wbp.[132] In particular, the APg noted that Black Box had no data security plan, retained data for an unnecessarily long period of time and did not inform data subjects. This led to the amendment of the SUWI Act and the Decree SUWI, and to the renaming of Black Box to SyRI.[133]

The above shows that the APg was and is involved with SyRI. However, it is unclear how far the involvement of the APg currently goes. It is, for example, unknown whether the Ministry of SZW still notifies the APg of every relevant project, or if the APg specifically monitors processing of personal data for separate intervention projects in SyRI. It is of the utmost importance that the APg closely monitors the use of SyRI. If such monitoring does not take place, detecting violations and misuse of the system will be very hard.

In addition, internal oversight is important. If an intervention team wants to start a SyRI project, the Minister must approve the application. If the Minister approves the application, the IB uses SyRI to combine and analyse several data sets. According to Article 5a.6.1 of the Decree SUWI, the Minister evaluates the risk model that the data controllers use for the analysis based on the feedback from the intervention teams. The approval by the Minister and the final evaluation are not subject to any further internal oversight.

Both internal and external oversight are considerably important to monitor whether data controllers, the Minister and intervention teams comply with the principles of data protection. Regarding the principle of lawful processing, oversight is necessary to make sure that the interferences and limitations remain justified and lawful, and that all the involved parties do not violate other human rights, such as the prohibition of discrimination.[134] In addition, effective oversight creates an extra check to prevent stigmatisation from happening, which in turn will have a positive influence on preventing discrimination. When profiling in order to obtain certain information, stigmatisation and consequently discrimination are real risks. It is easy to image certain social groups with less societal opportunities to be an easy target when they share the coincidence of living in a neighbourhood which is suspected to be inhabited by many persons committing social benefit fraud. As profiling or conduct related thereto are potentially dangerous methods, any such conduct should be under careful scrutiny in order to balance the possibility of biasedness, generalization and stigmatisation. With regard to the principle of purpose specification and limitation, oversight is necessary to determine whether personal data is really only used for the specified purpose and if this use is necessary and proportionate. Regarding the data quality principles, oversight is important to assess whether used personal data is always relevant, complete and correct. Additionally, oversight is necessary to determine whether controllers do not process personal data in secret, whether all the involved parties comply with their legal obligation of confidentiality and whether third

[131] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.
[132] Aanhangsel Handelingen 2014-2015, nr. 429, p. 4.
[133] *Kamerstukken II* 2012-2013, 33 579, nr. 4.
[134] EU Charter, Art. 21; ECHR, Art. 14.

parties do not have access to the personal data, thereby complying with the principle of fair processing.

If a controller does not comply with one of the data protection principles, a data subject must have access to a judicial remedy. Article 50(1) of the Wbp states that a data subject can request a judge in civil proceedings to forbid a controller to further process personal data, if this processing violates the principles found in the Wbp.[135] Furthermore, Article 49 of the Wbp states that a data subject can claim damages if processing has violated the principles found in the Wbp. It is unclear whether the use of SyRI qualifies as an appealable administrative decision.

[135] These principles follow from the EU and CoE legal framework and the principles as described in Chapter 3.

6. Conclusion

This research project focused on the application of SyRI and its compliance with principles of data protection. Two research questions formed the basis of the research. Firstly, the memorandum determined if and how SyRI complies with data protection principles that are derived from CoE and EU legislation. The research question underlying this part of the project was: 'To what extent does SyRI comply with data protection principles based on Council of Europe and European Union legislation?' Secondly, the focus shifted to a determination of the risks, if the answer to the first question was that SyRI does not comply with (a part of) a principle of data protection. The research question underlying this part of the project was: 'What are the risks that follow from (partial) noncompliance with data protection principles based on Council of Europe and European Union legislation?'

Intervention teams, consisting of several government institutions, can start investigation projects into a specific form of fraud in the Netherlands. This investigation starts with the creation of a risk notification by SyRI. SyRI creates this risk notification by combining different sets of personal data into profiles and comparing these profiles to a risk model, which is based on a number of pre-set indicators. Since SyRI processes personal data to create the risk analysis the system must comply with five data protection principles, which are based on CoE and EU legislation and case law. These principles are: the principle of lawful processing, the principle of purpose specification and limitation, data quality principles, the principle of fair processing and the principle of accountability. The analysis shows that SyRI complies with most of these principles.

The analysis of the principle of lawful processing leads to the conclusion that, although the use of SyRI constitutes an interference with the right to respect for private and family life and a limitation of the enjoyment of this same right and of the right to protection of personal data, it seems that this interference is justified and that the limitation is lawful. This in turn leads to the conclusion that the use of SyRI amounts to lawful processing.

The analysis of the principle of purpose specification and limitation shows that intervention teams have to specify the explicit purpose of every investigation project. The government and participating institutions have however not publicised documents explaining the purpose of projects, which makes it difficult to determine if this principle is really complied with.

The analysis of the data quality principles shows that SyRI may only use relevant and accurate data, which the data controller may only retain for a limited period of time. Since SyRI has access to a wide range of data it is questionable whether this data is always relevant for the detection of fraud. The fact that a SyRI project application must contain an explicit explanation regarding the use of specific data, may however balance this. It is also questionable whether the data is always accurate since SyRI relies on the different participating institutions for its data. It does seem however that the several safeguards and different steps in the procedure will filter out inaccurate data. SyRI furthermore only retains data for a limited amount of time.

The analysis of the principle of fair processing shows that the institutions and the government effectively inform the public of the start of project and its purpose through publications in several sources, but that the state of technological development may demand even more from the government. The analysis also shows that SyRI cannot process data in secret and that third parties do not have access to the used data.

The analysis of the principle of accountability shows that the APg must monitor if the controller of SyRI complies with the data protection principles. It is clear that the APg has been involved with SyRI. However, it is unclear to what extent the APg is currently involved and whether the APg closely monitors the conduct of the controller when using SyRI. In addition, the analysis shows that a remedy exists for individuals if a controller violates data protection principles and other rights of the individual.

Although the analysis shows that SyRI complies with most of the parts of the data protection principles, the analysis also shows that SyRI does not comply with some of the elements. This leads to the identification of the following risks.

With regard to the principle of purpose specification and limitation, a potential risk is the lack of transparency. As the government and participating institutions have not publicised specific applications of SyRI, it is not possible to assess the purpose of specific projects.

With regard to the data quality principles, the analysis shows that the use of numerous different sources by SyRI leads to the risk that data might not be relevant for the purpose of fraud detection. Although it is not a specific risk, it is also worrisome that SyRI uses data that was collected for very different purposes than fraud detection. Although the SUWI Act does seem to provide a legal basis for this use, individuals do not know of the further processing of their personal data.

With regard to the principle of fair processing the analysis shows that publications of information regarding the start of a new project do not contain information on the identity and address of the involved institutions. This makes it very difficult for an individual to determine which institution he or she has to contact for the provision of specific information regarding the processing of his or her personal data. The analysis also shows that no possibility exists for an individual to access his or her used personal data wherever the institution processes this data. An individual can therefore not object to the use of specific data.

With regard to the principle of accountability the analysis shows that it is unclear how far the involvement of the APg, as the external oversight body, currently goes and whether the APg closely monitors the conduct of the controller, and other involved parties such as the Minister, when using SyRI. It is of the utmost importance that the APg closely monitors the use of SyRI. If such monitoring does not take place, detecting violations and misuse of the system will be very hard. The same applies for internal oversight. The Minister evaluates the use of SyRI but no additional internal oversight, for example to monitor the conduct and decisions of the Minister, seems to take place.

7. Recommendations

- Request information from the government regarding themes and priorities set by the LSI to identify the purpose for the use of SyRI in specific years.

- Request information from the government regarding the approved applications for SyRI projects to identify:
    - specified purposes of approved projects;
    - relevancy of processed data;
    - accuracy of processed data.

- Request information from the government regarding the rejected applications for SyRI projects to identify:
    - type of projects that are rejected;
    - grounds for rejection.

- Request information from the government regarding the outcome of approved SyRI projects to identify weak and strong points following from the evaluations.

- Advise the government to notify individual citizens in a more effective and easily accessible manner about the start of intervention team projects.

- Advise the government to inform citizens that institutions may use their personal data, which was collected for a specific purpose, for fraud detection.

- Advise the government to include the address and identity of the relevant data controller when notifying the public of the start of an intervention team project.

- Advise the government to enable data subjects to access their personal data wherever it is processed.

- Advise the government to improve internal oversight to prevent discrimination and stigmatisation following from profiling.

- Advise the government to refer to the existing remedy under the Wbp in the SUWI Act or Decree SUWI.

- Advise the APg to publish information regarding the results of its oversight on the use of SyRI.