DEIKWIJS ADVOCATEN

SUBPOENA

Today, the _____, upon request of

1. The association with full legal competence **Nederlands Juristen Comité voor de Mensenrechten** ('Netherlands lawyers' committee for human rights', NJCM), established in (2311 GW) Leiden on Sterrenwachtlaan 11, in the following also referred to as 'NJCM',

2. The foundation **Stichting Platform Bescherming Burgerrechten** ('platform protection civil rights'), established in (1094 PW) Amsterdam on Ambonplein 73, in the following also referred to as 'Platform Bescherming Burgerrechten',

3. The foundation **Stichting Privacy First**, established in (1091 GR) Amsterdam on Wibautstraat 150, in the following also referred to as 'Privacy First',

4. The foundation **Stichting Koepel van DBC-vrije Praktijken van Psychotherapeuten en Psychiaters** (the organisation of psychotherapists and psychiatrists against the digital diagnostic register), established in Amsterdam with offices in (7371 EL) Loenen on Voorsterweg 153, in the following also referred to as 'Stichting KDVP',

5. **Landelijke Cliëntenraad** ('national clients' council'), established in (2594 AW) The Hague on Bezuidenhoutseweg 60, in the following also referred to as 'Landelijke Cliëntenraad',

6. Mr **Maxim Februari**,[1] residing in Buren,

7. Mr **Tommy David Wieringa**, residing in Waterland,

for the present case choosing domicile in (1019 AZ) Amsterdam on Panamalaan 8A at the offices of Deikwijs Advocaten, of which legal counsels A.H. Ekker and D.M. Linders are acting as lawyers in this case and are appointed as such,

I have,

SUBPOENAED:

The **STATE OF THE NETHERLANDS** ('Ministerie van Sociale Zaken en Werkgelegenheid', the Department of Social Affairs and Employment'), with seat in The Hague, serving my writ to the Attorney General at

[1] Maxim Februari is the pseudonym of Mr Maximiliaan Drenth.

the Netherlands Supreme Court 'Hoge Raad der Nederlanden' in (2511 EK) The Hague on Korte Voorhout 8 (in the following also referred to as the 'State') having served this writ and left copy of this writ:

☐ to: .....

☐ left in a closed envelope on which is stated the information prescribed by the law, because I did not find anyone there to whom I could legally leave a copy,

TO:

Appear on _____, of the morning at 10.00 AM, not in person, but represented by a lawyer, at the public civil hearing of the court of law of The Hague, which session will be held at such time and location in one of the chambers of the courthouse located in (2595 AJ) The Hague on Prins Clauslaan 60,

WITH NOTICE THAT:

- If the defendant fails to appoint a lawyer or does not timely settle the court fees indicated below, and on condition the prescribed terms and formalities have been observed, the court will judge on the defendant in absentia and rule in favour of the claim described in the following, unless it seems unlawful or unfounded to it;
- Upon appearance of defendant in the lawsuit, court fees will be levied which must be settled within four weeks counted from the time of appearance;
- The amount of the court fees is listed in the most recent annex associated with the law on court fees for civil cases 'Wet griffierechten burgerlijke zaken', which can be found on the website: https://www.kbvg.nl/griffierechtentabel;
- From a person without means will be levied court fees for the impecunious as established by or pursuant to the law, in case he has presented at the time when the court fees are levied:
    - a copy of the decision to grant legal assistance, as intended in article 29 of legal assistance legislation 'Wet op de rechtsbijstand', or if this is not possible as a result of circumstances which cannot reasonably be attributed to him, a copy of the application, as intended in article 24, second section, of said 'Wet op de rechtsbijstand', or otherwise
    - a statement of the board of the council for legal assistance 'raad voor rechtsbijstand', as intended in article 7, third section, part e, of said 'Wet op de rechtsbijstand' evincing that his income does not exceed the incomes intended in the general order in council pursuant to article 35, second section, of that law.

IN ORDER TO:

Respond to the following demands of complainants.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 At stake in the present proceedings is the call to cease the use by the Netherlands authorities of 'Systeem Risico Indicatie' ('SyRI' – 'risk indication system'), a risk-profiling system. SyRI is deployed under the responsibility of the Department of Social Affairs and Employment ('Ministerie van Sociale Zaken en Werkgelegenheid') with the intention, in brief, to prevent fraud in matters of social security, employment, and taxes. For this purpose, great quantities of personal data from various governmental data banks are linked and analysed. This leads to risk profiles of hundreds of thousands of citizens and, in some cases, to a so-called 'risk notification': a notification regarding an increased risk of illegitimate conduct or of non-compliance with labour laws.

1.2 SyRI affects the interests of all Dutch citizens, not only of those for whom risk notifications are reported. The sole authority, after all, to process personal data constitutes a limitation of the right to have one's privacy respected. In addition, anyone may be the object, without being aware, of the analyses which are conducted through SyRI.

1.3 The application of SyRI constitutes a violation of the right to protection of one's privacy and is in conflict with article 8 of the European Convention on Human Rights ('ECHR'). The legal arrangement on which the application of SyRI is founded, does not offer grounds to legitimise this breach. The use of SyRI must, therefore, be ceased and (parts of) the legal arrangement on which it is based must be declared non-binding.

1.4 The plaintiffs in this lawsuit acknowledge that the prevention of fraud in matters of social security, employment, and taxation may in itself be a legitimate objective. The system which the State of the Netherlands has designed to that effect, however, far overreaches such objective.

1.5 The legal arrangement for SyRI creates powers which may be deployed so broadly, that liberties are conferred to the authorities without hardly any limitation, to engage in large-scale data collection at own discretion, whereby the data of citizens are searched on the basis of secret risk models. Pursuant to the results of these, citizens may be included in a register and subjected to criminal and administrative sanctions by practically any governing body. In this manner, SyRI enables the authorities to meddle at random in the private lives of unsuspected citizens. The ECHR has ruled several times that the essential purpose of article 8 ECHR precisely is to protect the citizen against random interference by public authorities.[2]

1.6 The State attempts to legitimise the extremely extensive powers by an appeal to a 'broad limitation of purpose'. The principle of purpose limitation is an effect of the requirement of foreseeability as stipulated in article 8 ECHR.[3] This principle, however, demands that

[2] As in ECHR (Grand Chamber) 7 February 2012, 40660/08 and 60641/08 (Von Hannover v. Germany (No. 2)), r.o. 98.

[3] Conclusion of Advocate General J. Kokott of 18 July 2007, case C-275/06 (Promusicae), C-275/06, par. 53.

the purpose of data processing be formulated with the narrowest possible definition. Only in such case can it be determined whether the other principles of data protection legislation are complied with, such as the requirements of proportionality and data-minimisation as well as with the information obligation. A 'limitation of purpose which is as broad as possible' cannot fulfil this function. Data protection legislation must always be interpreted in accordance with article 8 ECHR.[4]

1.7 The data which is analysed by SyRI derive from sources which were never intended to be used for covert risk analyses. Any action on the part of the citizen vis-a-vis the authorities can thereby affect his legal position. This incrementing control through such shadow records damages the trust the citizen has in the authorities, has a *chilling effect* [term used in source – trnsltr] on his readiness to provide information to the authorities and thereby constitutes a fundamental threat to the Rule of Law. The State has never been able to demonstrate in an adequate manner the necessity of deploying SyRI. In addition, citizens are not informed of the data processing and cannot object to it. Also lacking is any type of independent scrutiny.

1.8 Over the past years, the European Court for Human Rights ('ECHR') and the European Court of Justice ('ECJ') has ruled repeatedly that the deployment of covert observation methods in the context of the detection and prevention of serious crimes and terrorism entailed a breach of the privacy of citizens. It is remarkable, in that perspective, that the State overrides all legal objections against the use of SyRI, including the legislative advice of the Netherlands high advisory council 'Raad van State' and the Board for data protection 'College Bescherming Personal data' ('CBP', in the meantime renamed 'Autoriteit Personal data'). The deployment of SyRI takes place without any concrete suspicion pertaining, and without the required assurances having been met.

1.9 The plaintiffs in this lawsuit – a coalition of civil society organisations and two concerned citizens, Maxim Februari and Tommy Wieringa – have attempted in various manners to bring their objections with regard to SyRI to the attention of the Department of Social Affairs and Employment ('Ministerie van Sociale Zaken en Werkgelegenheid') which is responsible for the deployment of SyRI. Unfortunately, to no avail so far. That is why the coalition deems it necessary now to file these main proceedings on substance byway of the Public Interest Litigation Project (PILP) of the 'Nederlands Juristen Comité voor de Mensenrechten' (the Netherlands Committee of Lawyers for Human Rights, NJCM).

2 LITIGANTS

2.1 The coalition of complainants consists of three civil society organisations and two citizens. The civil society organisations are all foundations which strive for the protection of

[4] 'Hoge Raad' 9 September 2011, ECLI:NL:HR:2011:BQ8097 (Santander), r.o. 3.3.

fundamental rights. They defend the public interest in the protection of the right to privacy of all Dutch citizens on grounds of article 3:305a BW (Civil Code).

2.2 NJCM strives, amongst other things, for 'the development, reinforcement, and protection of the fundamental rights and liberties of man at a national and international level', especially by promoting and enforcing 'the obligation of government to recognise the fundamental rights and liberties and to respect these in its actions and refraining from action', including by means of 'judicial and extrajudicial action if such is in the interest of the protection of the fundamental rights and liberties of man' (**Productie 1**).

2.3 The 'Platform Bescherming Burgerrechten' strives, amongst other things, for 'the protection of the inalienable possession of the classical civil rights, especially including the right to privacy' also by way of 'the conducting and/or supporting of test cases which are related to the preceding in the broadest sense or are conducive to such' (**Productie 2 below**).

2.4 Privacy First strives, amongst other things, for 'the maintaining and promotion of the right to privacy, as well as the personal freedom of living environment, in any manner whatsoever, for example by intervening judicially for all citizens in the Netherlands to protect this public interest and furthermore everything which is related to these matters directly or laterally or can be conducive to such, all things in the broadest sense of the term' (**Productie 3 below**).

2.5 The KDVP strives, amongst other matters, for 'the protection of and standing up for the privacy of the patients/clients of psycho-therapists, psychiatrists, and psychologists, standing up for the assurance of professional confidentiality as a fundamental legal obligation which is complementary to the privacy rights of patients/clients [… and] acting on behalf of stakeholders or groups of stakeholders falling within the objectives of the foundation as a litigant in the eligible professional and judicial […]' (**Productie 4**).

2.6 'Landelijke Cliëntenraad' is a consultative body for national client organisations and client councils and is the legal interlocutor of the Ministry in the context of policy developments and for the assurance of client participation. It strives to 'play an important part with regard to the contributions of clients to the policy fields of work and income, more specifically the labour market policy and re-integration policy, and the elaboration of client participation. 'Landelijke Cliëntenraad' offers a framework for integral involvement of the representative client organisations in the development of policy for people with entitlement to benefits and pensions and people with a handicap or chronic illness' (**Productie 5**).

2.7 Filing in addition in this lawsuit are two natural persons. Mr Maxim Februari is a philosopher, lawyer, writer, and columnist. His most recent novel, *Klont*, was released in 2017. He engaged in research of economics and ethics, resulting in a dissertation which was nominated for the literary prize 'De Gouden Uil'. For his literary oeuvre he was awarded the prize 'Frans Kellendonkprijs'. From 1999 to 2010 he wrote columns for the newspaper

'de Volkskrant', as from 2010 for newspaper 'NRC Handelsblad'. He took a stand against SyRI in a column of 7 October 2014 in 'NRC':

> *'The core objection against the control state or totalitarian state lies in the threat of government subduing and gagging you on grounds of such information. Berufsverbote, the denial of rights, accusations of violations which you are barely aware of having committed them.*
>
> *In such an abundance of data, after all, there is always something to find, especially if you are not searching for something specific. That is what the term phishing means in this context: if one starts snooping around in the life of a citizen, he will inevitably bump into something bad. In combination with the unreliability of the data, the unreliability of the systems and the unreliability, as referred to already, of the individual, this leads to an extremely unsafe society.'* (**Productie 6 below**)

2.8 Mr Tommy Wieringa is an author, columnist, and presenter. He wrote, amongst other things, the novels 'Joe Speedboot', 'Caesarion', and 'De heilige Rita'. For his penultimate novel 'Dit zijn de namen' he received the literary award 'Libris Literatuurprijs' 2013. In 2010, he wrote the text for the national dictation show 'Groot Dictee der Nederlandse Taal' and in 2014 he wrote the text for the national week-of-the-book gift 'Boeken-weekgeschenk'. In 2013, he presented the TV-series produced by broadcaster VPRO 'De Grens'. Journalistic work of him appeared in publications such as 'de Volkskrant', 'NRC Handelsblad', and 'Vrij Nederland'. Tommy Wieringa stated in his lecture 'Koesbroeklezing' of 1 April 2015 about SyRI, amongst other things:

> *'Municipalities, benefits implementing organisation UWV and the tax office already are enthusiastic users of SyRI, which they refer to as 'the washing machine'. It is in the belly of that machine that all citizens' data regarding labour, administrative measures and sanctions, detention, fiscal data, information about housing, civil integration, re-integration, debt burdens, benefits, permits, and health insurances disappear in. In brief, everything we share with the authorities, is combined and analysed by SyRI, so that deviations can be swiftly filtered. The old law which says that 'if it is technically feasible, it will be technically implemented', has given birth to an even uglier cub: 'What can be seen, will be seen.' [...] The alderman who dreamt of small checks now has at his disposal metadata which render the web of everyone's lives clearly visible to him – the dream of small checks has become the nightmare of complete transparency.'* (**Productie 7 below**)

2.9 Both Maxim Februari and Tommy Wieringa are Dutch citizens and have their regular residence in the Netherlands. As a result, both constantly run the risk at some point of falling under a SyRI risk profile and become the object of an investigation, even if they have not committed a violation of any legal regulation at all.

2.10 The State of the Netherlands is the defendant in these proceedings. The Department of Social Affairs and Employment ('Minister van Sociale Zaken en Werkgelegenheid') is responsible for the deployment of SyRI.

3 FACTS

Background SyRI

3.1 When SyRI was designed, the objectives and the consequences for the privacy of citizens were not carefully weighed against each other. In actual fact, SyRI is a continuation of a series of government projects for which a legal foundation was lacking. The initiative to realise a legal arrangement was an attempt to eliminate the objections of the advisory bodies of 'Raad van State' and CBP.

3.2 In 2003, the steering group 'Landelijke Stuurgroep Interventieteams' was founded. In it, various parties collaborate to fight undeclared work, illegal labour, social security fraud, and fiscal fraud. These partnerships were called intervention teams. In the intervention teams, the tax office 'Belastingdienst', labour inspection 'Arbeidsinspectie', social security implementers UWV and SVB, municipalities, the public prosecutor and the police collaborate.

3.3 Since 2006, the social intelligence detection service 'Sociale Inlichtingen- en Opsporingsdienst' ('SIOD') of the Department of Social Affairs and Employment 'Ministerie van Sociale Zaken en Werkgelegenheid' has experimented, jointly with the intervention teams, with risk profiles based on the linking of personal data deriving from various sources. Based on this, persons or businesses with an elevated risk of fraud could be selected.

3.4 In the memorandum on fraud prevention by linking files 'Notitie Fraudebestrijding door Bestandskoppeling' of 2006, the personal data watchdog CBP formulated a number of principles. For instance, CBP considers:

> *'Fraud prevention may not lead to a disproportional breach of the privacy of these citizens. What must be sought, therefore, is a balance between the interest of fraud prevention and the interest of protecting privacy. What must be prevented is that citizens who apply for or receive benefits are treated as potential frauds who may be checked without any limits. The rule of law means that a citizen is innocent until the contrary has been proven. Without a concrete suspicion of a violation of the*

law, the breach made of the privacy of the citizen, for example as a result of the linking of files, must be minimal.'[5] (**Productie 8**)

3.5 About the information obligation, CBP noted:

'The information obligation from article 34 WBP (data protection law) is applicable to the linking of files. CBP holds that in case of the standard linking in the context of the in-take, the proper provision of information concerning during the in-take interview is sufficient. In case of further checks by way of the linking of files, the risk group must be informed about thematic controls in a general sense before the actual check. This can be done, for example, by way of the information sheet of the social security agency. In case of the linking at an individual level flowing from the priorities of the enforcement policy, providing information beforehand indicating that the data of a benefits receiver may be checked by way of the linking of files cannot suffice. CBP holds that the social security agency must notify the person involved afterwards every time a benefits receiver is linked at an individual level, as to what files were matched. If detection and prosecution are proceeded with, the benefits receiver must be informed, in case the interest of the investigation allows such, of the activities which have led to this.'[6] (**Productie 8**)

3.6 In 2007, CBP drew an unfavourable conclusion after an internal investigation regarding a project whereby personal data about social welfare benefits were linked to water consumption in order to detect fraud regarding the housing situation of people with entitlement to social welfare benefits:

'After assessment of the linking of files "Waterproof' against these laws, CBP concludes that the data processing on this project is illegitimate. Personal data was requested from water companies and water authorities and linked to the records of municipalities, the tax office 'de Belastingdienst' and the social security implementer SVB while there were no grounds for this in the form of a suspicion of fraud or an elaborated risk analysis. This processing of data thus was not necessary in the sense of WBP and social benefits law WWB.

In addition, the processing of the data of the water authorities was incompatible with the purpose the data was obtained for by the water authorities. The provision of the data of the water supply companies and water authorities by the fraud prevention agency 'RCF-Noord' to 'Belastingdienst' and SVB violated the principle of

[5] CBP, 'Notitie Fraudebestrijding door bestandskoppeling', Den Haag: College Bescherming Personal data 2006, p. 1 (https://www.videnet.nl/download/?id=3863649).

[6] CBP, 'Notitie Fraudebestrijding door bestandskoppeling', Den Haag: College Bescherming Personal data 2006, p. 5 ff. (https://www.videnet.nl/download/?id=3863649).

the limitation of purpose. The data was used by municipalities, 'Belastingdienst' and SVB as a risk signal for further investigation.

Citizens who are checked through the linking of files have wrongly not been informed of this. As a result of "Waterproof", a type of processing of data has arisen which cannot be expected or comprehended for a major group of citizens who receive social benefits or rent allowance. In the paragraph 'assessment' of this letter, CBP indicates what considerations have led to the conclusion.'[7] (**Productie 9**)

3.7 In the Waterproof project, water consumptions data and the addresses of 35,000 citizens were requested from water suppliers with low water consumption as an indicator. These were subsequently linked to an address file of people entitled to social benefits. Ultimately it was established for 42 persons that cohabitation fraud was the case for them. This amounts to 1 in 833 citizens, or 0.12%.[8]

3.8 In response to the Waterproof report of CBP, then-undersecretary Aboutaleb conferred with CBP which advised, among other things, to start working with pre-prepared risk profiles.[9] Because the Department was not yet ready to do so, it was decided to proceed with the use of encryption of data by way of the so-called 'Black Box' method. By way of software, it would have been possible to link data in an 'anonymised' manner. Only the risk population would be rendered traceable and fed back to the client.

3.9 In 2011, following an internal investigation, CBP imposed an order subject to a penalty on SIOD on account of a Black Box project. SIOD overran the retention periods, saved data for purposes which had not been established beforehand, and had not secured data sufficiently. In addition, SIOD failed to adequately inform those involved. The contention of SIOD that it did not have to inform due to the interest of the prevention, detection, and prosecution of criminal acts was rejected by CBP. Article 43 of the law on the protection of personal data 'Wet bescherming personal data' ('Wbp'), which under certain circumstances creates the possibility to leave unapplied rights of those involved, must be applied in a restrictive manner. Furthermore, it should have been assessed per case whether and for how long an appeal to the grounds for refusal was justified. A general appeal to the exception did not suffice.[10]

---

[7] CBP, 'Bevindingen ambtshalve onderzoek Waterproof', Den Haag: College Bescherming Personal data 2007, p. 2 (https://autoriteitpersonal data.nl/sites/default/files/downloads/uit/z2006-00476.pdf).

[8] Inspectie SZW, 'Nota van bevindingen, Bestandskoppelingen bij fraudebestrijding', Den Haag: Inspectie Sociale Zekerheid en Werkgelegenheid 2012, p. 21 en 22 (https://www.inspectieszw.nl/binaries/inspectieszw/documenten/rapporten/2012/06/15/bestandskoppelingen-bij-fraudebestrijding/Bestandskoppeling-bij-fraudebestrijding.pdf).

[9] *Kamerstukken II*, 2007–2008, 17 050, nr. 346, p. 2 (Letter of the undersecretary of the Department of Social Affairs to the Chairman of Parliament).

[10] CBP, 'Besluit tot oplegging last onder dwangsom', Den Haag: College Bescherming Personal data 2011, p. 9 (https://autoriteitpersonal data.nl/sites/default/files/downloads/pb/pb_20110317_siod_lod_besluit.pdf).

3.10 On a SyRI-project in Groningen in 2013, the data of 119,000 people entitled to benefits were linked to cadastral information. Ultimately, for 117 persons illegitimacy and/or fraud was established (1 in 1017 or 0.098%) and for 10 persons benefits were terminated (1 in 11.900 or 0.008%).[11]

3.11 The enforcement actions by CBP have apparently convinced the State in the end – on 1 January 2013 – that a specific legal arrangement was required for the linking of files and the drawing up and using of risk profiles. This arrangement is contained in article 64 and 65 of the law on the structure of the implementation organisation for work and income 'Wet structuur uitvoeringsorganisatie werk en inkomen' ('Wet SUWI') and chapter 5.a of the associated decree 'Besluit SUWI'.

3.12 In the legislative process, both the advisory legal council 'Raad van State' and the personal data watchdog CBP issued quite critical advice. Raad van State concluded that the purpose of SyRI was too broad and too vague and could not serve as the purpose for the processing of personal data in the sense of said law Wbp. The wide description of purpose left leeway for data processing which serves a non-legitimate purpose and was in conflict with the requirements of purpose limitation and compatible use. According to 'Raad van State', the system could be too easily expanded towards bodies without an exact description and citizens wrongly were not informed of the processing and provision of their personal data (**Productie 10 and Productie 11**).

3.13 CBP concluded that the necessity of the deployment of SyRI had not been substantiated with a concrete, substantive weighing of interests and that it was insufficiently clear how risk indicators would be deployed for the selection of personal data. The principle of '*select before you collect*' had not been complied with. The collection of personal data without a necessity substantiated beforehand and without established and objectified risk indicators would lead to '*fishing expeditions*' and arbitrariness (**Productie 12**, p. 4). In addition, the information obligation in Wbp was not complied with. It was also unclear according to CBP on what legal grounds the processing of data within SyRI was based on (**Productie 13**, p. 5).

3.14 The advice of 'Raad van State' and CBP were shrugged off for the most by the State, or solely addressed in the most cosmetic of manners.

[11] Inspectie SZW, 'Nota van bevindingen, Bestandskoppelingen bij fraudebestrijding', Den Haag: Inspectie Sociale Zaken en Werkgelegenheid 2012, p. 22 (https://www.inspectieszw.nl/binaries/inspectieszw/documenten/rapporten/2012/06/15/bestandskoppelingen-bij-fraudebestrijding/Bestandskoppeling-bij-fraudebestrijding.pdf).

Law and Decree SUWI and application of SyRI

3.15 Article 64 and 65 'Wet SUWI' and 'Besluit SUWI' make it possible that administrative bodies, municipalities, and the Department of Social Affairs and Employment engage in partnerships, that they exchange personal data within those partnerships and have that personal data analysed by SyRI. The legislative texts are submitted as **Productie 14** and **Productie 15**.

3.16 If two or more administrative bodies decide to enter into a partnership with the purpose (in brief) of preventing fraud with social benefits or taxes, they could be constrained as a result to provide each other with information (article 64 section 3 'Wet SUWI'). If they decide to request the deployment of SyRI from the Department, then they are also obliged on grounds of such request to provide the data to the Department (article 64 section 4 'Wet SUWI'). On account of this request, the Department is subsequently obliged to process this data in SyRI and acts for the processing of data as data controller in the sense of said Wbp (article 65 section 1 'Wet SUWI').

3.17 Included in the request to the Department must be, amongst other things, what administrative bodies and persons are collaborating, what the objectives of the partnership are, how it is organised, when the project would preferably start, and who supplies the data. It must also be evinced what indicators and what risk model the request is in regard to (article 5a.1 section 2 'Besluit SUWI'). Finally, it must be evinced by the request that each administrative body:

a. Has assessed the intended provision of files against the data which is required for the risk analyses, for the benefit of the purpose of the SyRI-project, including the purpose in article 64 section 1;

b. Has substantiated that the processing of the data with regard to the interests of the (legal) persons is not disproportional relative to the purpose;

c. Only provides that data which is required for the risk analyses; and

d. Cannot achieve the same goal in a less drastic manner (article 5a.1 section 4 'Besluit SUWI').

3.18 If the request meets the conditions, the Department determines the commencing date of the SyRI-project and announces it in the official gazette 'Staatscourant' (article 5a.4 section 1 'Besluit SUWI'). The data processing is effectively carried out by the 'foundation intelligence agency', 'stichting Inlichtingbureau' ('Inlichtingenbureau'), a private party acting under the responsibility of the Department and acting in that context pursuant to article 5a.2 section 2 'Besluit SUWI' as 'processor' in the sense of Wbp. Inlichtingenbureau aggregates the supplied files, encrypts and pseudonymises the data and subsequently links them in accordance with a risk model established by the Department (article 5a.2 section 3 and 5a.1 section 7 'Besluit SUWI'). The risk model consists of a number of

indicators on grounds of which it should become apparent whether an increased risk of irregularities pertains.

3.19 Subsequently, 'Inlichtingbureau' decrypts that data which, based on the results of the linking with the risk model, indicates an 'increased risk of irregularities as intended in article 64 section 1 "Wet SUWI"'. That data is aggregated in a file which is provided to the Department. 'Inlichtingenbureau' subsequently destroys all files within four weeks (article 5a.2 section 4 'Besluit SUWI').

3.20 The Department analyses the results and assesses what cases constitute grounds for a risk notification (article 5a.3 section 1 'Besluit SUWI'). The Department provides the partnership which filed the application with the risk notifications which are required for the proper execution of the task which is theirs pursuant to the Law. A risk notification is described as 'the provision in name from SyRI containing the identification of an increased risk of illegitimate use of government funds and government facilities and of which the risk analysis is a part' (article 65 section 2 'Wet SUWI' iuncto. article 1.1 sub z 'Besluit SUWI'). The Department destroys the data of (legal) persons which does not constitute grounds for a risk notification within four weeks after the analysis (article 5a.3 section 3 'Besluit SUWI').

3.21 There is a risk notifications register in which 'data regarding risk notifications' is directly included in order to inform project participants and administrative bodies on the risk notifications which were issued and to inform the subjects of risk notifications upon request whether their data is included in the register (article 5a.5 section 1 and section 5 'Besluit SUWI'). The data which is required for the purposes of the risk notifications register must be provided to project participants and subjects of projects (article 5a.5 section 3 'Besluit SUWI'). The arrangement does not require, however, for those involved to be individually informed of the risk notifications after conclusion of the investigation (article 5a.5 section 4 'Besluit SUWI'). The data regarding the risk notifications is retained until two years after the risk notification was inserted in the register (article 5a.5 section 5 'Besluit SUWI').

3.22 The administrative bodies can carry out a further investigation in response to a risk notification for a period of two years. The results of this investigation must be communicated to the Department within twenty months after the start of the SyRI-project (article 65 section 6 'Wet SUWI' and article 5a.3 section 4 'Besluit SUWI'). This feedback contains for example, if available, the results of the risk notification, its usefulness and, in case a risk notification has not led to follow-up action, the reason for this (article 5a.6 section 2 'Besluit SUWI'). The feedback also announces the end of the SyRI-project, unless the Department decides on this at another time (article 5a.4 section 2 'Besluit SUWI'). After the feedback, though no later than two years after the start of the SyRI-project, all data obtained within the framework of the project must be destroyed by the Department (article 5a.3 section 5 'Besluit SUWI'). If data, at any time, is destroyed, an authenticated report must be prepared for this (article 5a.7 'Besluit SUWI').

Prior history

3.23 Before these proceedings, the complainants have submitted a request on 12 December 2016 to obtain information pursuant to article 3 section 1 'Wet openbaarheid van bestuur' (the law stipulating the transparency of governance, 'Wob') (**Productie 16**). This information request aimed to acquire insight into the manner in which SyRI is applied in practice. The request regarded information concerning, e.g.:

a. All partnerships in the sense of article 64 section 1 'Wet SUWI' and intervention team projects whereby SyRI was deployed, both prior to the entry into effect of 'Wet SUWI', and in the subsequent period;

b. Information about the implementation and the results of all individual projects, including the substantiation of the necessity per project, the risk models and indicators established per project, the processed data and a summary of the costs incurred, the number of fraud cases effectively detected, and the enforcement measures effectively deployed against them;

c. A statement of the number of registrations in the Register risk notifications.

3.24 The Department honoured the Wob-request, but by far exceeded the decision term of eight weeks as established in Wob. On 8 March 2017, the first partial ruling was issued, on 6 June 2017 the second, and on 5 July 2017 the third. The partial rulings are submitted as **Productie 17**, **Productie 18** and **Productie 19**. All Wob-documents provided on the basis of those partial rulings have been published on-line by the Department.[12]

3.25 The information and documents ultimately provided by the Department regard, otherwise than as requested by complainants, exclusively the period after the entry into effect of article 64 and 65 'Wet SUWI' and therefore only regard three projects: 'G.AL.O.P. II Eindhoven', 'Capelle aan de Ijssel' and 'pilot Adresfraude Afrikaanderwijk Rotterdam'. Since October 2013, therefore, only three projects have been started. All three of these projects have not yet been completed. In the project 'Afrikaanderwijk', in addition, the deployment of SyRI was renounced due to capacity issues (**Productie 17**, p. 4).

3.26 In addition, the information and documents provided do not offer the clarity desired with regard to the application of SyRI. A part of the questions posed by the complainants has not been answered. It is not evinced by the supplied documents, for example (i) how much the projects referred to have cost, (ii) how many cases of illegitimate use, fraud, or non-compliance have in total been detected and (iii) what amount in fraud has been

[12] https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri and https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/07/05/besluit-wob-verzoeken-over-syri. In case of reference to Wob-documents in this subpoena, the numbering as included in the inventory list of partial ruling 1 (Productie 17) is consistently maintained.

prevented or detected in total. In conclusion, the Department refuses to grant the perusal of the risk models and indicators used (**Productie 17**, p. 3).

3.27 The documents provided by the Department have given insufficient clarification and have not lifted the objections brought to the fore by the complainants. In response to a request to that effect from complainants, consultations have taken place on 15 January 2018, also in the context of article 3:305a section 2 BW (Civil Code), at the Department of Social Affairs and Employment ('Ministerie van SZW'). During these consultations, the civil servants involved indicated that the Department does not agree with the objections of complainants and that it will not take any measures to eliminate these objections (**Productie 20**).

4 LEGAL FRAMEWORK

4.1 Complainants appeal to the right to the protection of one's private life, the protection of privacy, and the protection of personal data as laid down in article 8 ECHR, article 7 and 8 of the Charter of the Fundamental Rights of the European Union ('Charter'), article 17 of the International Covenant on Civil and Political Rights ('ICCPR') and the implementation of those rights in community and national legislation, especially Wbp and the General Data Protection Regulation (2016/679, 'GDPR'). In addition, complainants appeal to the right to an '*effective remedy*' and the right to a fair trial, as stipulated in articles 6 and 13 ECHR, article 47 Charter, and article 14 ICCPR.

4.2 Limitations of these fundamental rights, as in 'Wet SUWI', must respect the substantive content of those fundamental rights, states article 52 Charter.

4.3 To the extent the Charter contains rights which correspond with rights from ECHR, the content and scope thereof are the same as those attributed thereto by ECHR (article 52, section 3 Charter). Wherever reference is made without any further clarification to article 8 ECHR, thereby is also intended article 7 and 8 Charter and article 17 ICCPR. All these articles have direct legal force in the Netherlands legal order and are a part of Netherlands legislation pursuant to the articles 93 and 94 of the Netherlands Constitution.

Protection of privacy and of personal data

4.4 The articles 8 ECHR, article 7 and 8 of the Charter and article 17 of the ICCPR consecutively state:

> Article 8 ECHR – Right to the honouring of private life family life
>
> 1. Everyone has the right to respect for his private life and family life, his home and his correspondence.

2. No interference from any public authority is permitted in the exercise of this right, otherwise than provided for by law and as is necessary in a democratic society in the interest of national security, public safety, or the economic wellbeing of the country, the prevention of disorder and criminal acts, the protection of health or common decency or for the protection of the rights and liberties of others.

Article 7 Charter – Honouring of private life and of family life

Everyone has the right to respect for his private life, his family life, his home and his communications.

Article 8 Charter – Protection of personal data

1. Everyone Has the right to the protection of the personal data concerning him.

2. This data must be honestly processed, for certain purposes and with the consent of the data subject or pursuant other legitimate grounds provided for by the law. Everyone has the right of access to the data collected on him and to the rectification thereof.

3. An independent authority monitors the observance of these rules.

Article 17 ICCPR

1. No one may be subjected to arbitrary or unlawful interference in his private life, his family life, his home, and his correspondence, nor to the unlawful violation of his honour and reputation.

2. Everyone has the right to protection by the law against such interference or violation.

4.5 Limitations to fundamental rights by the authorities, as in 'Wet SUWI', on grounds of ECHR must meet three conditions: (i) the powers proposed must be sufficiently knowable and foreseeable for citizens, and the deployment of the proposed powers must be provided with sufficient safeguards to protect their rights, (ii) the limitation must be necessary in relation to the established purpose and this necessity must be sufficiently substantiated, and (iii) there must be a situation of effective and independent supervision of the deployment of the powers.

Foreseeability

4.6 It flows from article 8 section 2 ECHR, that the limitations to the right to respect for one's privacy must be arranged for by law ('*prescribed by law*'). The ECHR has implemented this requirement in several rulings:

> *'Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be*

able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.'[13]

'The law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence'[14]

4.7 Legislation must, therefore, be *accessible*, *foreseeable*, *and sufficiently precise* and contain sufficient safeguards against abuse and arbitrariness to thus provide individuals with an adequate indication of the circumstances and conditions under which the authorities may deploy the measures.[15] The result of that assessment depends, amongst other things, on *'the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.'*[16] The ECHR thereby requires detailed rules: *'the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity'*.[17]

4.8 In case of covert oversight, the law must additionally describe in what circumstances and under what conditions public bodies have the power to exercise such covert oversight. In addition, in such case a number of specific conditions must be complied with. In matters regarding covert surveillance by intelligence services, the ECHR has established that it must be clear:

a. What activities or violations may be grounds for oversight;

b. What categories of persons can be subjected to powers of oversight;

c. What the maximum duration is of the powers of oversight;

d. What procedure must be followed to be able to investigate, use, and save the obtained data;

e. What precautionary measures must be taken in case of the use of the data and the provision thereof to third parties; and

[13] ECHR 26 April 1979, 6538/74 (Sunday Times), r.o. 49.

[14] ECHR 24 April 1990, 11105/84 (Kruslin Huvig), r.o. 29.

[15] ECHR 12 May 2000, 35394/97 (Khan), par. 26; ECHR 2 September 2010, 35623/05 (Uzun), par. 61; ECHR 29 June 2006, 54934/00 (Weber and Saravia), par. 93; ECHR 1 July 2008, 58243/00 (Liberty et alia), par. 62.

[16] ECHR 2 September 2010, 35623/05 (Uzun), par. 63; EHRM 29 June 2006, 54934/00 (Weber en Saravia), par. 106, ECHR 2 August 1984, 8691/79 (Malone), r.o. 68, EHRM 26 September 1995, 17851/91 (Vogt), r.o. 48.

[17] ECHR 29 June 2006, 54934/00 (Weber and Saravia), par. 94; EHRM 1 July 2008, 58243/00 (Liberty e.a.), par. 62.

f. The circumstances under which the data must be deleted or destroyed.[18]

4.9 In the opinion of complainants, these safeguards must apply equally in case of covert and computerised data-analyses such as by way of SyRI. After all, thereby a much more intrusive picture can be sketched of the private life of a citizen than by way of surveillance.

Requirement of necessity

4.10 On grounds of article 8 section 2 ECHR, a limitation of the right to have one's privacy respected in addition must be necessary in a democratic society. A breach of a fundamental right is only permitted in the event of a legitimate purpose and a *pressing social need* and on condition the requirements of proportionality and subsidiarity are met.

4.11 The prevention of, in brief, social security and tax fraud can be designated as a legitimate purpose under ECHR. The breach must be effectively necessary with an eye on this legitimate purpose. A weighing of interest will, therefore, have to be conducted every time as to whether the deployment of SyRI is effectively required, whereby all relevant circumstances must be taken into consideration. The circumstance that for data processing an appeal can be made to a legal foundation does not render superfluous this weighing of interests.[19]

4.12 The requirement of necessity only concerns the concrete deployment of powers. Also the introduction of new powers in itself must be necessary in a democratic society. It flows from jurisprudence of ECHR and ECJ that the simple existence of legislation already on grounds of which personal data can be processed counts as a breach of the protection of privacy.[20]

Oversight in matters regarding article 8 ECHR, article 13 ECHR

4.13 In case of the secret processing of personal data, citizens are not aware of the limitation of their rights. As a result, they do not have the possibility in practice to present any possible violations to the court of law. As is apparent from the rulings of ECHR the condition applies in such case that there must be a situation od adequate and effective guarantees against the abuse of powers by the authorities.

---

[18] See EHRM 29 June 2006, 54934/00 (Weber en Saravia), par. 95 and the rulings referred to there; ECHR (Grand Chamber) 4 December 2015, 47143/06 (Zakharov v. Russia), r.o. 227 ff. and EHRM 12 January 2016, 37138/14 (Szabó & Vissy v. Hungary), r.o. 56 e.v.

[19] 'Hoge Raad' (Supreme Court) 9 September 2011, ECLI:NL:HR:2011:BQ8097 (Santander), r.o. 3.3.

[20] ECHR (Grand Chambers) 4 December 2015, 47143/06 (Roman Zakharov), r.o. 168-171; EHRM 6 September 1978, 5029/71 (Klass e.a.), par. 41; ECJ (Grote Kamer) 8 April 2014, case C-293/12 (Digital Rights Ireland) r.o. 32 and ECJ (Grand Chambers) 21 December 2016, case C-698/15 en C-203/15 (Tele2 Sverige/ Post och telestyrelsen). Also see: S. Eskens, O. van Daalen & N. van Eijk, 'Ten standards for oversight and transparency of national intelligence services', Amsterdam: Institute for Information Law (University of Amsterdam), 2015, p. 14.

4.14 An important means of preventing abuse is to guarantee effective and independent oversight. An independent institution must control whether the authorities operate within the boundaries of their powers, on grounds of the correct procedures, and with due regard for the requirements of proportionality and subsidiarity. This oversight must be effective pursuant to article 13 ECHR and the scope thereof must therefore include all stages of the exercise of powers.

4.15 Oversight must preferably be exercised by the court of law.[21] An alternative to judicial review, however, is only acceptable in the event of a combination of both internal and external safeguards. These guarantees may consist, e.g., of '*internal control, parliamentary oversight, independent oversight, and a complaint procedure before an independent body*'.[22] Prior authorisation by an independent institution is not sufficient in itself. There must also be legitimacy oversight *after-the-fac*t on the implementation of the operation and the manner in which the authorities concretise the necessity assessment. On grounds of article 13 ECHR, it must be possible for this legitimacy oversight to result in a binding ruling.

Article 6 ECHR

4.16 In article 6 ECHR, the right to a fair trial has been established:

> Article 6. Right to a fair trial
>
> 1. When determining his civil rights and obligations or when determining the legitimacy of such prosecution he is subjected to, everyone has the right to the fair and public handling of his case, within a reasonable term, by an independent and impartial court established by the law. The sentence must be pronounced in public but access to the courtroom may be denied to the press and the public, during the entire trial or a part thereof, in the interest of common decency, of public order or national security in a democratic society, if the interest of minors or the protection of the private life of litigants require such, or, to such extent as is deemed strictly necessary by the court under special circumstances, in the event the public character would impair the interests of the proper application of justice.
>
> 2. Anyone who is subject to prosecution is considered innocent until his guilt has been judicially established.
>
> 3. Anyone who is subject to prosecution, specifically has the following rights:
>
> a. to be informed forthwith, in a language he understands and in particulars, of the nature and reasons of the accusation brought to bear against him;

[21] ECHR 6 September 1978, 5029/71 (Klass e.a.), par. 56 and ECHR 18 May 2010, 26839/05 (Kennedy t. VK), par. 167.

[22] S. Eskens, O. van Daalen & N. van Eijk, 'Ten standards for oversight and transparency of national intelligence services', Amsterdam: Institute for Information Law (University of Amsterdam), 2015, p. 16.

[…]

4.17 In this context a distinction must be made between disputes or procedures in which only civil rights and obligations are addressed on the one hand, and situations of prosecution with a *criminal charge* in the sense of article 6 section 2 ECHR on the other. It is important thereby, that the scope of article 6 ECHR is very broad. By civil rights and obligations are covered practically all disputes in the field of civil law. In addition, prosecution does not pertain merely in case of a criminal suspicion, but also in case of disputes and procedures regarding administrative violations and sanctions, such as violations of social security legislation and the granting of fiscal allowances.[23] It is furthermore important that article 6 ECHR is applicable to all stages of the trial, also the preceding, preparatory stages in which the treatment of the case or prosecution do not formally pertain yet.

4.18 A number of rights can be derived from article 6 ECHR, including the right of access to an independent and impartial judge, the right to a fair trial and *equality of arms* and the so-called presumption of innocence.

Community and national legislation

4.19 The constitutional protection of privacy as laid down in the ECHR, the Charter, and the ICCPR, has been further elaborated at a community and national level in a number of principles of data protection legislation. At the moment of the subpoena, the most important legal source in the context of these proceedings is the EU Privacy Directive (95/46/EC) which was implemented in the Netherlands through Wbp. On 24 May 2016, however, GDPR has come into effect. GDPR is directly applicable as from 25 May 2018. At that moment, the Privacy Directive and Wbp come to lapse. The present case will, therefore, have to be decided on for all data processing in SyRI from that date onwards on the basis of the relevant provisions in the GDPR. In the following, the relevant principles will be discussed on the basis of the GDPR, whereby reference will also be made each time to the relevant clauses in the Privacy Directive ('Rl') and Wbp.

Necessity and proportionality

4.20 Article 6 section 1 GDPR (article 7 Rl and 8 Wbp) contains the community application of the requirement of necessity. In it is established that the processing of personal data must be required on grounds of one of the legal bases for processing indicated there.

Requirement of legal basis

[23] ECHR 25 August 1987, 9912/82 (Lutz), r.o. 54; ECHR 23 October 1995, 15523/89 (Schmautzer), r.o. 27/28; ECHR 23 September 1998, 68/1997/852/1059 (Malige), r.o. 35/36; ECHR 4 March 2008, 11529/02 (Hüseyin Turan), r.o. 17-19; ECHR 23 November 2006, 73053/01 (Jussila), r.o. 30-32.

4.21 The requirement of legal basis is established in GDPR in article 6 (article 7 Rl and 8 Wbp). Personal data may only be processed if one of the six legal bases pertains:

a. The data subject has given his consent;

b. The processing is required for the implementation of an agreement to which the data subject is a party, or to take measures before conclusion of an agreement upon request of the data subject;

c. The processing is required to comply with a legal obligation which the data controller is subject to;

d. The processing is required to protect the vital interests of the data subject or of another natural person;

e. The processing is required for the fulfilment of a task of public interest or of a task in the context of the exercise of the public authority with which the data controller has been charged;

f. The processing is required to defend the legitimate interests of the data controller or of a third party, except in case the interest or the fundamental rights and the fundamental liberties of the data subject which demand the protection of personal data outweigh those interests, especially in case the data subject is a child.

4.22 Article 6 section 2 GDPR establishes that the legal foundation sub f) does not apply for the processing by government institutions in the context of the exercise of their tasks. The legal foundations for processing referred to sub a), b) and d) are not applicable either. For SyRI, therefore, only sub c) or sub e) could apply as a legal basis for processing.

Limitation of purpose

4.23 Article 5 section 1 sub b GDPR establishes that personal data must be collected for well-established, expressly described and legitimate purposes and must not be further processed in a manner incompatible with those purposes (article 6 section 1 sub b Rl and 7 Wbp). The purpose must be established prior to the data processing and it must be clear and specific, so it is clear what types of processing are covered by it and which are not. Purposes which are formulated in too vague and general a manner do not qualify as sufficiently well-established.

4.24 The limitation of purpose can be seen as a special form of foreseeability and constitutes a cornerstone of data protection legislation.[24] The limitation of purpose is stipulated as an explicit condition in article 8 of the Charter.

[24] Conclusion of Advocate General J. Kokott of 18 July 2007, case C-275/06 (Promusicae), C-275/06, par. 53.

4.25 Article 6 section 4 GDPR (article 9 Wbp) stipulates that if the processing for another purpose than that for which the personal data was collected is not founded on the consent of the data subject, that the data controller for the assessment of the question whether the processing for another purpose is compatible with the purpose for which the personal data was originally collected, must take into account matters such as:

a. Any relationship between the purposes for which the personal data was collected and the purposes of the intended further processing;

b. The framework within which the personal data was collected, especially as regards the relationship between the data subjects and the data controller;

c. The nature of the personal data, especially whether special categories of personal data is processed and whether personal data regarding criminal convictions and criminal offences is processed;

d. The possible consequences of the intended further processing for the data subjects;

e. The existence of appropriate safeguards, possibly including encryption or pseudonymisation.

Computerised decision-making and profiling

4.26 In GDPR, standards are included regarding profiling. The term profiling is defined in article 4 part 4 GDPR as:

> *'any form of computerised processing of personal data whereby, based on personal data, certain personal aspects of a natural person are evaluated, especially with the intention to analyse or predict his professional performances, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.'*

4.27 Pursuant to article 21 section 1 GDPR, a data subject has the right at all times to object on account of reasons related to his specific situation against processing which takes place on grounds of article 6 section 1 sub e or f, including against profiling.

4.28 The data subject in addition has the right not to be subjected to a decision based exclusively on computerised processing, including profiling, associated with legal consequences for him or which affect him otherwise to a substantial degree (article 22 section 1 GDPR, article 15 Rl and article 42 Wbp).

Information obligation

4.29 The data controller is obliged to adequately inform data subjects on the processing of their personal data (article 13 and 14 GDPR, article 11 Rl and article 33 and 34 Wbp). If personal data was not obtained from the data subject, the data controller must provide the following information:

a. The identity and the contact details of the data controller;

b. In such case as may occur, the contact details of the data protection officer;

c. The processing purposes the personal data is intended for, and the legal basis for the processing;

d. The categories of personal data involved;

e. The receivers of the personal data.

4.30 In addition, the data controller must provide the data subject with the following information to assure proper and transparent processing (article 14 section 2 GDPR):

a. The period during which the personal data will be stored, or if such is not possible the criteria to determine that term;

b. The legitimate interests of the data controller if the processing takes place pursuant to article 6 section 1 sub f GDPR;

c. That the data subject has the right to request the data controller for the perusal and rectification or deletion of personal data or to limit the processing regarding him, as well as to object against processing and to the transferability of data;

d. That the data subject has the right to submit a complaint to the monitoring authority;

e. The source the personal data derives from and in such case as may occur whether it derives from public sources;

f. The existence of computerised decision-making, also including the profiling intended in article 22, sections 1 and 4, and, at least in such cases, useful information about the underlying rationale, as well as the importance and expected consequences of that processing for the data subject.

4.31 The data controller must provide the information on grounds of section 3:

a. Within a reasonable term, but no later than within one month after obtaining the personal data, depending on the concrete circumstances in which the personal data is processed;

b. If the personal data will be used for communications with the data subject, no later than at the time of first contact with the data subject; or

c. If the provision of the data to another receiver is being considered, no later than at the time when the personal data will be provided for the first time.

4.32 On grounds of section 4, the data controller, in case he has the intention to further process the personal data for another purpose than the one the personal data was obtained

for, must provide the data subject before such further processing with information about that other purpose and all relevant further information as intended in section 2.

Processor agreement

4.33 A controller can have the processing of personal data carried out by a third party. This third party will in such case be designated as a 'processor' (article 4 part 8 GDPR/article 1 sub e Wbp).[25] The controller is obliged pursuant to article 28 section 3 GDPR (article 14 section 2 Wbp) to arrange for the processing of personal data by a processor in an agreement or through another legal transaction. This article section prescribes what conditions a processor agreement must meet. It must be established, for example, that the processor exclusively processes personal data on the basis of written instructions from the controller, that he takes adequate technical security measures, and that he takes the required measures in the event of a data leak.

4.34 If no processor agreement has been concluded, it is unlawful to have personal data processed by a processor.

Non-disclosure obligations

4.35 The data which is used within SyRI derive from a great number of varying administrative bodies. For these administrative bodies, varying legal non-disclosure obligations apply. Article 74 'Wet SUWI' and article 65 'Participatiewet' (participation law) establish, for example, that 'it is prohibited to all to further disclose what becomes known or is communicated to him in connection with any activity upon the implementation of this law about the person or affairs of someone else, than what is required for the implementation of this law or is prescribed or permitted on grounds of this law'. This non-disclosure obligation is applicable, for example, to the tax office 'de Belastingdienst'. For 'de Belastingdienst' applies besides the specific legal non-disclosure obligation of article 67 of the general law regarding national taxes 'Algemene Wet inzake de Rijksbelastingen' ('Awr'). In conclusion, there also exists a general legal obligation for administrative bodies to treat personal data of citizens in a confidential manner, laid down in article 2:5 of the general administrative law 'Algemene wet bestuursrecht' ('Awb').

5 VIOLATIONS BY THE STATE

5.1 Article 64 and 65 of 'Wet SUWI', the decree 'Besluit SUWI' based on it, and the deployment of SyRI in itself are in conflict with ECHR, the Charter, the ICCPR, the Privacy Directive, the GDPR, and Wbp. Through the deployment of SyRI the State also violates several non-disclosure obligations. These violations do not merely entail the meddling in

[25] The law on personal data protection Wbp still refers to an 'editor'. The meaning of this concept is identical.

the private lives of citizens, but besides they damage the trust of the Dutch citizen in the Netherlands authorities and the rule of law. The existence of far-reaching powers to covertly link all sorts of government databases creates the feeling among citizens that they are constantly monitored by the authorities.

5.2 In these proceedings, Complainants wish to submit the legal arrangement for SyRI for assessment against the provisions of treaties which are binding for all. Conflict with provisions of treaties which are binding for all entails that the regulations in case must be left inapplicable (article 94 Constitution). For this assessment, the rulings of international courts, such as the ECHR and the ECJ, must be observed. The declaration to be left inapplicable is in effect until such condition as may be included in an application prohibition, such as the modification of components of the law so that the violation of fundamental rights was to be lifted.

5.3 If your court were to judge that application of article 64 and 65 of 'Wet SUWI', 'Besluit SUWI' and/or any components thereof are in conflict with the fundamental rights mentioned in this subpoena, thereby the unlawful action (article 6:162 BW – Civil Law) of the State vis-à-vis Complainants and vis-à-vis anyone whose interests they defend has been established.

5.4 That a substantial and far-reaching limitation of the right to privacy pertains is evident. For great numbers of innocent citizens, big quantities of, partially sensitive, data is collected, saved, exchanged between government institutions, linked and used for the drawing up of profiles and the preparation of risk analyses. Data for which the citizen could not have foreseen in any way that it was going to be used for this purpose. ECHR has judged that even the saving of personal data constitutes a limitation of the right to have one's privacy protected, regardless of the use which is subsequently made of that data.[26] In case of SyRI, the citizen is at risk of being included in a criminal register and to be stigmatised as a result.

Unforeseeable/Legal foundation is lacking

5.5 The legal arrangement for SyRI does not meet the foreseeability requirement in several respects.

Description of purpose too broad

5.6 In the first place, the description of purpose in article 64 section 1 'Wet SUWI' is formulated too broadly and vaguely and thereby not 'sufficiently precise'. The State, in response to highly principled criticism from the government's legal advisory board 'Raad

[26] ECHR (Grand Chamber) 4 December 2008, 30562/04 and 30566/04 (S. and Marper), r.o. 67.

van State' (see **Productie 10**) has merely made some cosmetic additions in the Explanatory Memorandum.

5.7 The description of purpose regards arrangements which cover entire policy fields: social security, labour laws, illegal labour, social security contributions and taxes including allowances.[27] In response to this criticism from 'Raad van State', the State has concretised the listing in the sense that in the Explanatory Memorandum, now a number of specific laws is mentioned.[28] That can hardly be termed a further delimitation, however. In addition, the government remarks in the Further Report ('Nader Rapport'):

> *'What was chosen for is a (broad) limitation of purpose which covers the domain of the Departments of Social Affairs and Employment and that of Finance.'*[29]
>
> *'In addition, the expansion of administrative bodies and persons enabled by Ministerial Decree, will always regard the monitoring of compliance or the implementation of other laws than those already mentioned.'*[30] [underscored by lawyer]

5.8 So thereby the State has opened the door for the designation of other laws by ministerial decree which may fall within the scope of the arrangement. Despite the advice of 'Raad van State', the legislator has chosen in addition to have such transpire by ministerial decree and not through a general order in council.[31]

5.9 It is important furthermore, that the legislator ultimately leaves assessment in concrete cases to the collaborating administrative bodies. 'Raad van State' remarked regarding:

> *'Such an assessment in concrete cases has a value in itself, but it does not relieve the legislator of the obligation to describe the attribution of administrative powers and the limitation of fundamental rights entailed by such as concretely as possible. The proposal does establish that within a partnership personal data is processed which, for the purpose discussed above, is required for that partnership. This description does not provide either, in the opinion of the Section, a delimitation of the purpose of the processing of data. It is thereby furthermore unclear whether the participants in the partnership for the processing of data is bound in that context by the powers they have at their disposal pursuant to other laws and by the*

[27] *Kamerstukken II* 2012-2013, 33 579, no. 4, p. 2 and 3 (Advice 'Raad van State' (RvS) and 'Nader Rapport' (Further Report')).

[28] *Kamerstukken II*, 2012-2013, 33579, no. 3, p. 36 and 37 ('Memorie van Toelichting', Explanatory Memorandum).

[29] *Kamerstukken II*, 2012-2013, 33579, no. 4, p. 5 (Advice RvS and 'Nader Rapport').

[30] *Kamerstukken II*, 2012-2013, 33579, no. 4, p. 7 (Advice RvS and 'Nader Rapport').

[31] *Kamerstukken II*, 2012-2013, 33579, no. 4, p. 7 (Advice RvS and 'Nader Rapport').

purposes for which those powers were attributed to them, or that the proposal creates an independent legal basis for the processing of data.'[32]

5.10 The government set aside this criticism completely. The description of purpose was 'chosen broadly deliberately':

'A broad limitation of purpose was deliberately chosen to achieve that the administrative bodies and persons that collaborate in practice can also effectively act as integral authorities against illegitimate use, fraud, and non-compliance with legislation. The citizen also wants this from the authorities. This entails that the purpose of the collaboration must be broad.' [33]

5.11 A 'wide' or 'broad' limitation of purpose is a *contradictio in terminis*. The principle of the limitation of purpose demands that a purpose is well-determined, expressly described, and justified. The requirement of being well-determined means that the purpose must be described with sufficient detail to assure compliance with the law and to demonstrate data protection safeguards, as is explained as well by the article 29 working group 'Artikel 29-Werkgroep'[34] (**Productie 21**, p. 15). As a result of a 'broad limitation of purpose', foreseeability is at issue. Besides, the required proportionality cannot be properly assessed.

5.12 So beforehand, the individual hardly has any indication of the situations in which he may become subject to a far-reaching intrusion in his privacy. The fields in which SyRI can be deployed are very broad and for a substantial part delimited only in a vague manner. The concretisation thereof takes place at the level of the executive power. At that moment, it is too late for the unsuspecting and well-intentioned citizen. A certain combination of actions (and associated registrations), which each in itself does not have to constitute the violation of any regulation, can all of a sudden fall within a certain risk profile.

5.13 The description of purpose in addition contains a number of terms which are not precisely delineated. It is not clear, for instance, what must be understood by 'unlawful use of government funds and government facilities'. Is thereby only intended that government funds are collected while one is not entitled to them, or also that government funds are effectively 'used' unlawfully? If the latter applies, the scope of it has no limits. In addition, by 'unlawful use' is referred, according to toe explanatory memorandum, to both:

'the incorrect use and to the deliberately incorrect use (abuse) of government funds and government facilities in the field of social security and income-dependent arrangements.'[35]

---

[32] *Kamerstukken II*, 2012-2013, 33579, no. 4, p. 3 (Advice RvS and 'Nader Rapport').

[33] *Kamerstukken II*, 2012-2013, 33579, no. 3, p. 36 ('Memorie van Toelichting').

[34] 'Artikel 29-werkgroep' is the independent advisory and consultation body of European privacy watchdogs.

[35] *Kamerstukken II* 2012-2013, 33 579, no. 3, p. 36 ('Memorie van Toelichting' – explanatory memorandum).

5.14 Incorrect use, however, does not by definition have to be unlawful, as in the case it is not attributable. The term 'unlawful use' is broader than the term 'abuse', because it also includes lighter violations, whereby intent is lacking. The application of SyRI even seems possible outside the domain of criminal and unlawful actions, considering what is stipulated in article 5a.2. section 3 sub f 'Besluit SUWI'. This clause already renders possible the processing of data in the event of 'an increased risk of irregularities'.

5.15 The description of purpose applied is intended to enable the broadest possible application of SyRI and as a result does not offer Dutch citizens the protection which is needed based on the applicable constitutional and privacy law standards.

5.16 Considering the preceding, the citizen who has provided his data to the authorities in a number of separate relationships is confronted with a type of processing of his data which is covert and opaque and the underlying rationale for which and the possible consequences of which he cannot know.

5.17 In the end, the administrative bodies responsible for a SyRI project do not concretely formulate a description of purpose which eliminates the legal latitude and vagueness. The descriptions of purpose in the three projects which have been started since the entry into effect of the legal arrangement of SyRI, are just as vague and broad and besides for a big part do not even fit within the description of purpose of article 64 section 1 'Wet SUWI'.[36] This evinces that – to the extent article 64 'Wet SUWI' contains any delimitation of the description of purpose – the administrative bodies in SyRI-projects implement such in their own manner to a high degree. In the project proposal Afrikaanderwijk is even formulated as the central objective 'the improvement of the quality and reliability of the civil registry Basisregistratie Personen'. That purpose can in no manner be made to be included in the description of purpose of article 64 section 1 'Wet SUWI'.

Competence not delineated

5.18 In the second place, the formulation of the power to deploy SyRI in article 64 and 65 'Wet SUWI' does not meet the requirement of foreseeability. The obligation of sharing data within a partnership arises as soon as an administrative body 'decides to participate in a partnership' (article 64 section 3 'Wet SUWI'). The obligation to provide data to the Department arises as soon as the partnership makes a request for the conducting of risk analyses (article 64 section 4 'Wet SUWI').

[36] See for the project GALOP II: the request for application SyRI in Wob-document 2, can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 4/16; for the project Adresfraude Afrikaanderwijk Rotterdam: the project proposal in Wob-document 24, can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 5/16 and for the project Wijkgerichte aanpak kwetsbare buurten Capelle aan den IJssel: the project proposal in Wob-document 40, can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 6/16.

5.19 The arising of said 'obligations' is thereby exclusively based on the subjective decision of the relevant administrative bodies and persons to participate in a partnership or in a request for the carrying out of a risk analysis. The consideration which must assure that the deployment of SyRI is foreseeable, necessary, proportional, and subsidiary, has not been implemented in the legal arrangement, but according to the legislator is a task of the administrative bodies involved in a SyRI-investigation, which must establish whether the processing of data provided by them is subsidiary and proportional.

5.20 Thus, it is not delineated in any manner under what circumstances or based on what considerations these administrative bodies and persons can make such a decision. 'Wet SUWI' and 'Besluit SUWI' do not offer any objective criteria on the basis of which citizens can estimate under what circumstances data processing may be proceeded with.[37] Article 64 section 3 and section 4 'Wet SUWI' offer, in other words, a practically unlimited possibility for the processing of data, while the requirement of foreseeability aims, on the other hand, for the very delineation of the powers of the authorities.

5.21 In 'Wet SUWI', the powers are formulated in such a broad manner, that the degree of limitation is largely dependent on the choices made by the executive parties. In this manner, practically all personal data which citizens provide to the authorities (most of the time compulsorily) is used against them by way of an unforeseeable and uncontrollable method. This occurs in a manner which is not established in the legislative text but is determined per project by the parties which on account of their tasks pursuant to the law have an interest in the same risk profiling. This has an undermining effect on the relationship of trust between citizens and the authorities, as a result of which the most important safeguard for open communications from citizens towards the authorities are badly damaged.

5.22 It is evinced by the Wob-documents that it does not become clear in the actual projects how the weighing of interests by the relevant administrative bodies has transpired. In the project proposal GALOP II, the advice request from LSI, the advice from LSI, and the final approval by the Department, no substantiation whatsoever can be found for the necessity of the project, a weighing of interests relative to the breach of privacy, or the data to be processed, of the risk models or of the possible consequences of a risk notification. It does not go beyond the generalities such as that 'the proposal meets the legal requirements'.[38] The same applies to the project Capelle.[39]

---

[37] Cf. ECJ (Grand Chamber) 8 April 2014, case C-293/12 (Digital Rights Ireland), r.o. 59-60 and 65.

[38] See Wob-documents 1 to 4, which can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 4/16.

[39] See Wob-documents 40 to 54, which can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 6/16.

5.23 In addition, it is evinced by the Wob-documentation that, for instance, the duration of the deployment of powers is insufficiently upheld. The project GALOP II should have run until 15 October 2016, after extension until 1 June 2017.[40] The project Capelle should have run until 15 April 2017.[41] In each case, at the time of the third partial ruling of 5 July 2017, both projects had not been completed yet (**Productie 19**).

Data categories too vague and too broad

5.24 In the third place, the listing of data categories which is eligible for processing in SyRI is too broad. The ruling lists 17 categories of personal data which can be processed (art 5a.1. section 3 'Besluit SUWI'). It regards, in brief:

a. Employment information;
b. Information regarding measures and sanctions in the field of administrative law;
c. Fiscal information;
d. Information on movable and immovable property;
e. Information on grounds for exclusion of benefits or social security;
f. Trade information;
g. Housing information;
h. Identifying information, being in case of a natural person: name, address, place of residence, mail address, date of birth, gender, and administrative characteristics;
i. Civil integration details, being information by which it can be determined whether civil integration obligations have been imposed on a person;
j. Compliance information;
k. Educational information;
l. Pension information;
m. Re-integration information;
n. Debt burden information;
o. Benefits, allowance and subsidy information;
p. Permits and exemptions; and
q. Health insurance information.

5.25 The description of the listed categories is very broad and comprehensive each time. Because the purposes for processing are formulated in such a broad manner, the necessity

[40] See Wob-document 10, which can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 4/16.

[41] See Wob-documents 45 and 46, which can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 6/16.

of the use of this information is, furthermore, impossible to determine. In its advice on 'Besluit SUWI' 'Raad van State' remarks the following in this context:

> *'The listing of information may be intended to limit the processing of data (principle of data minimisation) but in actual fact is so broad, that hardly any personal data can be thought of which is not eligible for processing. The list does not seem to be intended to limit, but to create as much leeway as possible. Even if for each individual project it will be further established what data is necessary for such project – as the Section also remarked in its advice on the legislative proposal on which the draft decree is based – such assessment in concrete cases does not relieve the legislator (and the issuer of the decree in this case) of the obligation to describe the attribution of administrative powers and the associated limitation of fundamental rights in as concrete a manner as possible.'*[42] (**Productie 11**, p. 5)

5.26 In view of the preceding, the Section has advised to critically review the categories of personal data for necessity, subsidiarity, and proportionality, and to focus the description in the draft decree on what is in correspondence with those requirements. The government has persisted in its position, however, that the scope of the data to be processed is only established per project. The objection of 'Raad van State', therefore, has not been lifted.

5.27 It is furthermore evinced by the Wob-documents that it is kept a secret what data is ultimately processed within a project. All projects started so far under the current legal arrangement make use of data in conformity with the risk model 'Wijkgerichte Aanpak' ('district-based approach', WGA).[43] That risk model is kept secret (**Productie 17**, p. 3), so it is and remains unknown what personal data exactly is processed on this project. The model seems to be so secret, that even the participating administrative bodies do not know what data it regards exactly.[44]

Risk models are secret

5.28 In the fourth place, it remains unforeseeable for the citizen at all times how SyRI will be deployed in a specific project, because the risk models remain secret. Complainants have asked in their Wob-request to be provided with this risk model. This part of the Wob-request was rejected:

---

[42] Raad van State, Advice W12.14.0102/III, https://www.raadvanstate.nl/adviezen/advies.html?id=11339, p. 2.

[43] GALOP II: Wob-document 2 (under 2b and 2d) can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 4/16; Afrikaanderwijk: Wob-document 27 (under 2b and 2d), can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 5/16; Capelle: Wob-document 44 (under 2b and 2d), can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 6/16.

[44] E-mail exchange of 7 and 17 August 2015 in Wob-document 22, p. 16 and 17, can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/07/05/besluit-wob-verzoeken-over-syri, file 5/5.

'I note that a risk model is a collection of one or more sets of interrelated risk indicators which jointly provide an estimate of the risk that certain natural or legal persons do not act in accordance with the law. By disclosing what data and relationships the Department's inspection ("Inspectie SZW") concentrates on, (potential) infringers can know exactly what registrations they must focus on.

[…]

In view of the preceding, for the document with sequence number 76, the interest of the detection and prosecution of criminal offenses and the interest of inspection, control, and oversight by "Inspectie SZW" is at stake. I hold that this interest, consisting of the conducting, free from impediments and possible outside influence, of investigations by 'Inspectie SZW' must outweigh the (public) interest of transparency. I have therefore decided not to disclose the information in case.' (**Productie 17**, p. 3)

5.29 So the risk model which is used to analyse the collection of data is not disclosed at all. This is objectionable in the first place because the risk model cannot be assessed in this manner, for example against the ban on discrimination (also see marginal nos. 5.44). Discrimination based on risk models is an obvious risk. A possible distinction between various groups of citizens must be objectively justified and open to assessment against verifiable information.[45] In the second place, citizens cannot gauge in any manner when a risk notification may be made.

5.30 Those risk models must be disclosed just as well based on article 14 section 2 sub g and article 22 section 1 GDPR, read in conjunction with consideration 71. In case of SyRI, both computerised decision-making and profiling take place. For the definition of profiling, for that matter, it is not required that a computerised decision also takes place. To the extent the computerised decision-making and profiling by way of SyRI even were permitted under article 22 GDPR, the underlying rationale of it must in any case be rendered public (**Productie 22**, p. 7, 8, 13 and 14).

5.31 Finally, computerised decision-making based on data in a 'black box' leads to an unequal trial position, which is incompatible with art. 6 ECHR. This is evinced by a recent ruling by the section administrative law ('Afdeling Bestuursrechtspraak') of 'Raad van State', in which the Section considered:

'The PAS, the associated appropriate assessment and AERIUS, however, also entail the risk that the partially computerised decision-making on grounds thereof is not transparent and controllable due to a lack of insight into the choices made and the data and presuppositions used. If stakeholders wish to utilise legal instruments

[45] CRvB 13 June 2017, ECLI:NL:CRVB:2017:2481, r.o. 4.5.4 ff.; CRvB 27 November 2017, ECLI:NL:CRVB:2017:4068, r.o. 4.5 ff.

against decisions based on PAS, an unequal trial position of parties may arise as a result. In case of decision-making based on a program which from their perspective can be considered a so-called 'black box', they cannot control, after all, on what basis a certain decision is reached and whether there is certainty that the project or other actions will impair the natural characteristics of Natura 2000-areas.

14.4. To prevent this unequal trial position, the Secretaries and Undersecretary referred to are under the obligation to render public the choices made and the data and presuppositions used entirely, timely, and voluntarily, in an appropriate manner, so that these choices, data, and presuppositions are accessible to third parties. This full, timely, and adequate provision must make it possible to assess or have assess the choices made and the data and presuppositions used and, if necessary, to challenge them in a substantiated manner, so that effective legal protection against decisions which are based on these choices, data, and presuppositions is possible, whereby the court will be able to assess the legality of these decisions on such basis.'[46]

No legal basis for processing

5.32 For the processing of personal data through SyRi, the legal basis for processing is lacking. This applies to both (i) the provision of data by administrative bodies to other parties within a partnership, including by the tax office 'de Belastingdienst', (ii) the provision of data by the Department to the intelligence agency 'Inlichtingenbureau', and (iii) the further processing within SyRI by the Department.

5.33 For SyRI, only the legal foundations sub c) of sub e) of article 6 section 1 GDPR (article 7 RI and 8 Wbp) are eligible. The legal obligation which the State has wanted to create in article 64 section 3 and section 4 'Wet SUWI', however, does not comply, for the reasons mentioned above (see marginal number 5.3 ff.), with the requirement of foreseeability and for this reason cannot apply as a legal obligation in the sense of sub c). Furthermore, this obligation is entirely dependent on the subjective decision of the administrative bodies themselves to form a partnership. Also CBP expressed criticism regarding:

> *'Pursuant to article 64, first section, of 'Wet SUWI' (new), the Department (as data controller) processes upon joint request of the administrative bodies and persons mentioned in the third section, data in SARI* [name originally chosen for SyRI – lawyer]*. This regards a legal obligation for the Department as data controller and thus data processing in the sense of article 8, heading and under c, of Wbp. However, within the context of this proposal processing of data takes place by other controllers besides. The administrative bodies and/or persons mentioned above, after all, supply personal data to the Department pursuant to article 64 of "Wet SUWI" (new). CBP does not understand how a joint request of these administrative*

[46] Raad van State 17 May 2017, ECLI:NL:RVS:2017:1259, r.o. 14.4.

bodies and/or persons to the Department can be designated as a "legal obligation" in the sense of article 8, heading and under c, of Wbp.'[47] (**Productie 12**, p. 5, in this context also see **Productie 13**, p. 5)

5.34 The processing of data cannot be based either on a legitimate interest in the sense of article 6 section 1 sub f GDPR. Article 6 section 1 GDPR establishes, after all, that part f does not apply to the processing of personal data by government institutions within the context of the exercise of their tasks. Also under Wbp it applies that the processing of data through SyRi, considering the scope and sensitive character thereof, cannot be founded on this basis. Also the legal basis for processing sub e) cannot serve as a basis for SyRI, in the first place because the objective aimed for through the deployment of SyRI cannot be classified under the interests indicated there, and in the second place because the requirement of necessity as laid down sub e) is not met.

5.35 'Raad van State' and CBP wondered as well whether the government tried to create a new legal basis or that an appeal was made to an existing legal basis or to compatible use. To this, the government has not offered an answer (**Productie 10**, p. 3 and 4 and **Productie 13**, p. 5).

No necessity

5.36 In order to be compliant with article 8 ECHR, the State must substantiate the necessity of the deployment of SyRI by way of a concrete, substantive weighing of interests, in accordance with the principle of proportionality and subsidiarity. It must be possible to justify intrusion with a factually demonstrated '*pressing social need*'. CBP already noted before the adoption of the legal arrangement, that this has not transpired for any of the individual measures:

'The intended linking of files through SARI, after all, cannot be substantiated through the general knowledge that abuses exist in the field of social security and the statement that SARI 'has an added value'. This knowledge does not render legitimate the limitation based on a 'pressing social need'. A 'pressing social need' must be substantiated by facts. In addition, it must be rendered plausible that the proposed measure provides for this pressing social need. Finally, the proposed measure must be weighed against the right to have the private lives of those involved respected. None of the proposed measures are substantiated by a weighing of interests, whereby the consequences of the legislative proposal for the privacy of the citizen compared to the current situation are weighed. For the substantiation of the necessity of linking personal data through SARI, it is requested in particular to dedicate attention to the circumstance that in the proposed system, the risk

[47] Cbp, 'Advies inzake effectiever gebruik van gegevens', The Hague: CBP 2012, p. 5.

notifications do not have to be investigated further by the receiving institutions, as this weakens the necessity of the linking.' (**Productie 12**, p. 3)

5.37 With regard to the principle of proportionality, CBP notes in its advice on the draft decree SyRI as follows:

> *'The intention to prepare profiles based on negative personal traits (debts, detention, violations, sanctions, fraud signals, etc.) on the basis of which risk notifications for the purpose of fraud prevention will be provided to the administrative bodies and persons, sheds a particular light on the proportionality of potential data processing through SyRI. This is not addressed in the proposal, with the result that no proper weighing of proportionality can be conducted. As a result, the risk pertains that the privacy interests of data subjects are impaired more than is necessary, and therefore disproportionately.'* (**Productie 13**, p. 4)

5.38 In addition, the assessment of the proportionality is problematic, precisely because the purposes which are served by SyRI have been formulated so broadly ('broad limitation of purpose'). The assessment of whether the means are in proportion to the purpose requires the delineation of the purpose with some degree of precision.

5.39 To substantiate the necessity, the government argues that in 2011, social security fraud for an amount of € 153 was identified. SyRI would play a substantial part in the fight against this fraud, as the completed intervention projects until 2010 have jointly yielded over € 23 million.[48] This substantiation is insufficient in itself to conclude that the deployment of SyRI is necessary. In the first place, it is not clear what the costs have been for the deployment of SyRI, so that the actual net yield cannot be determined. In response to the Wob-request submitted by Complainants, the Department indicates that there is no insight into the costs incurred per partner. As it is, costs incurred through the deployment of project hours are not specifically labelled but a part of the regular work process, days the Department (**Productie 19**, p. 3).

5.40 An assessment of the proportionality can in the second place only be made on the basis of specific information about the nature and scope of the processing of data and about the limitation of privacy which this processing entails, which the Department does not seem to have taken into consideration at all.

5.41 Relevant in the first place is the number of citizens which is subject to the processing of data. For the intervention projects completed until 2010, however, no figures are available which provide insight thereinto.[49] Also with regard to the projects G.A.L.O.P. II and

---

[48] *Kamerstukken II* 2012-2013, 33 579, no. 3, p. 17 ('Memorie van Toelichting').

[49] Questions of the MPs Gesthuizen and Ulenbelt (both SP) to the Secretary of Safety and Justice ('Staatssecretaris van Veiligheid en Justitie') and the Secretary of Social Affairs and Employment about the news that the Department of Social Affairs possibly violated privacy legislation (submitted 6 October 2014), Aanhangsel Handelingen 2014-

Capelle, the Department has indicated explicitly 'that the number of citizens is not known, because data is only saved in the event of a risk notification' (**Productie 19**, p. 3). The only relevant information until now is that on the project Capelle, in the end 137 risk notifications were issued (**Productie 17**, p. 4). The State, in brief, has not been able to determine for any of the projects, either those already implemented or the current ones, how many citizens were subject to them. The conclusion that the deployment of SyRI is proportional, is unfounded for this reason alone. A public discussion about the desirability and the proportionality of the deployment of SyRI is also impossible due to the lack of adequate information regarding the scope of the processing of data.

What must be taken into consideration is that SyRI is not only an infringement on the privacy of citizens with regard to whom a risk notification is made. After all, all Dutch citizens can become the subject, without being aware, of profiling within a SyRI-project.

5.42 In the second place, for the assessment of proportionality the nature and gravity of the infringement must be considered. The nature of the data which is combined in SyRI varies from public information, such as a Chamber of Commerce registration, to information about detention, debt burdens, illness histories, and detailed consumption of electricity by way of the smart meter. Sensitive and partially intimate information which certainly in combination create a detailed picture of someone's private life. This information touches on the essence of respect for one's private life. This applies all the more as the access to this information depends merely on the subjective decision to enter into a partnership by the administrative bodies and persons mentioned in article 64 'Wet SUWI'. As a result, such access is unconditional and general. The preceding means that the limitation to the right to the protection of one's privacy cannot be remediated by way of procedural safeguards alone. The State has unjustly not taken into consideration the sensitivity of the data which is processed SyRI for the assessment of proportionality.

5.43 In addition, the infringement is not merely limited to the forwarding of data by the parties to a partnership, but also consists of the processing by 'Inlichtingenbureau' and 'Inspectie SZW', and the possible insertion in the register risk notifications.

5.44 What should weigh heavily as well that there is an issue of profiling in the sense of article 4 sub 4 GDPR. For the persons subject to it, profiling entails varied risks, such as the risk of wrong decisions as a result of erroneous or obsolete data and stigmatisation and discrimination on account of being a part of a certain group. When using SyRI such risk can arise already before an administrative body would decide on further investigation or actual law enforcement. It is easy to image, in this manner, that in a small municipality the

2015, no. 428 and question of MPs Van Weyenberg and Schouw (both D66) to the Department ('Minister van Sociale Zaken en Werkgelegenheid') about the news «Sociale Zaken overtrad mogelijk de privacywetgeving» (submitted 7 October 2014).

sole existence of a risk notification with regard to a certain person or a certain family leads to stigmatisation among the civil servants who are confronted with the risk notification.

5.45 In conclusion, it is important that the exchange of data within SyRI constitutes a large-scale breach of the principle of purpose limitation. Use is made of data which the citizen has provided within the confidential relationship with the authorities. The application of systems such as SyRI entails a major and harmful *chilling effect*. Citizens no longer trust their own authorities and will tend less and less to provide their data.

5.46 The actual effect on the privacy of data subjects can only be evaluated by assessing the proportionality of the total processing of data. The State has failed to implement such an integral assessment.

5.47 The legal arrangement for SyRI does not provide either for such integral assessment of SyRI-projects by partnerships. It must be evinced by a request to start a SyRI-project that each of the administrative bodies and persons within a partnership 'has substantiated that a possible violation of the interests of the natural persons or legal persons which the processing of data is in regard to, is not disproportionate relative to the purpose which is aimed for with the deployment of SyRI' (article 5a.1 section 4 'Besluit SUWI'). This regulation does not eliminate the objections indicated above. Because it regards here, as is apparent from the formulation of this clause, a consideration which the parties involved must all make for themselves concerning the data supplied by them. The impact of the data processing within a SyRI-project, however, is bigger than the sum of the separate supplies. Furthermore, each SyRI-project comprises a number of other steps which are quite determinant as well for the impact on privacy, including the drawing up of risk models and the subsequent processing of data by 'Inlichtingenbureau'. Finally, the potential consequences for individual citizens must be taken into consideration, which is not a part of the requirements either. It is evinced by the Wob-documents, furthermore, that administrative bodies in practice do not engage in this weighing of interests at all, or at least not that we can know of.[50]

Conflict with the requirement of purpose limitation and compatible use

Limitation of purpose in 'Wet SyRI' and 'Besluit SyRI'

5.48 The limitation if purpose protects the interests of citizens by establishing boundaries to the way in which data is processed. 'Article 29-Werkgroep', the most important European

[50] GALOP II: Wob-document 2 (under 2b and 2d) can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 4/16; Afrikaanderwijk: Wob-document 27 (under 2b and 2d), can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 5/16; Capelle: Wob-document 44 (under 2b and 2d), can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 6/16.

advisory body in the field of privacy, formulates the importance of the limitation of purpose as follows:

> *'When we share personal data with others, we usually have an expectation about the purposes for which the data will be used. There is a value in honouring these expectations and preserving trust and legal certainty, which is why purpose limitation is such an important safeguard, a cornerstone of data protection. Indeed, the principle of purpose limitation inhibits 'mission creep', which could otherwise give rise to the usage of the available personal data beyond the purposes for which it was initially collected.'* (**Productie 21**, p. 4)

5.49 As noted above, the legislator has expressly chosen for a broad description of purpose in article 64 section 1 'Wet SUWI'. This description of purpose is not sufficiently well-determined, as is required by article 5 section 1 sub b GDPR and for this reason is in conflict with the principle laid out in it. To substantiate this, reference is made for brevity to marginal numbers 5.6 to 5.17.

5.50 The data which the partnerships may aggregate based on the relinquishing of the criterium of purpose limitation, are obtained for the most part pursuant to a specific legal basis. This specific legal basis constitutes the foundation for the control of the power of government. That is why purpose limitation may not be cancelled in a general sense or 'broadened' into something which it is not, without at least a demonstrable suspicion pertaining that the data subject is guilty of a weighty abuse or crime, and the intervention of the judiciary is at hand as well.

5.51 The justification for the obligatory provision of data to the authorities on the one hand lies in the necessity for the government entity to use this data in its executive practice, but on the other hand in the fact that the use of this data by this one party does not entail a major infringement on the liberty of the citizen. In case the data which is obtained by all individual parties is aggregated and used against the citizen, then the liberty of the citizen is in great peril. The protection of public interests by the authorities should never be at the expense of the public interest of protecting the citizen against the abuse of power by those very authorities.[51]

Further use incompatible

5.52 The processing of personal data within SyRi must be assessed against the criteria for compatible use, as formulated in article 6 section 4 sub a to e GDPR. This applies to (i) the provision of data by administrative bodies and other parties within a partnership, including by the tax office, (ii) the provision of data to 'Inlichtingenbureau' and (iii) the further processing within SyRI.

[51] Nardell QC G., 'Levelling up: Data Privacy and the European Court of Human Rights', In: Gutwirth S., Poullet Y., De Hert P. (eds), *Data Protection in a Profiled World*. Springer: Dordrecht 2010, p. 45.

5.53 Because the purpose of SyRI and the categories of data to be processed are described broadly and vaguely, it is difficult to adequately assess the compatibility with the original purposes. This in itself is objectionable already.

5.54 The explanatory memorandum 'Memorie van Toelichting' to Wbp states with regard to the requirement of purpose limitation in case of the linking of files by the authorities as follows:

> *'An example is the comparison of the detainees file and the file of the receivers of social security benefits. In case there is no entitlement to benefits in case of detention, both files can be compared with the result that any possible hits are communicated to the relevant implementation body of social security. It is not necessary, to that effect, that the penitentiary institutions take cognisance of the file of benefits receivers or the implementation bodies of social security take cognisance of the entire detainees' records. Such must be prevented, then, by way of technical and organisational measures. The provision of hits to the relevant implementation body is justified in such case through the assignment to apply the criteria for the granting of benefits. In this case, the purpose of the linking manifests such close relatedness to the original purpose for which the implementation body acquired the data, that – also considering the provisions which were taken to keep the distribution of data to the absolute minimum required – compatible use can be said to pertain. Different is the situation in which linking takes place for a purpose which is relatively far removed from the purpose for which the data was collected. In such case – separate from the linking which may find their legal basis in article 43 – incompatible use can be said to pertain much sooner.'*[52] [underscored by lawyer]

5.55 It must be concluded based on the criteria for compatibility in article 6 section 4 GDPR, that the use of personal data in SyRI cannot be compatible with the original purposes for which this data was collected.

5.56 There is no relatedness between the original purpose of processing and the purpose of data processing in the context of SyRI. All categories of data which are mentioned in 'Besluit SUWI' regard data which was collected by governing bodies for the purpose of specific public tasks, such as the imposition of taxes or the implementation of social security legislation. The relevant data is relevant and necessary in that relationship for the exercise of the tasks of such governing body. The use of the data referred to in the context of covert profiling, however, regards an entirely different situation. The citizen is not directly a part hereto, while this processing of data may, however, negatively affect him in his interests.

5.57 As regards the nature of the data (article 6 section 4 sub b GDPR), it must be concluded that it regards a considerable number of broadly described categories of data which

[52] *Kamerstukken II*, 1997-1998, 25 892, no. 3, p. 94 ('Memorie van Toelichting').

(partially) concern sensitive personal data. In some cases, it even regards special personal data which fall under the specific legal regime of article 16 Wbp. The categories as stated in article 5a.1 'Besluit SUWI' are partially formulated in an open manner (see e.g. sub d, e, j) so that potentially practically all data which bodies maintain within these domains can be deployed for SyRI, including data with regard to criminal convictions and data concerning health. All these categories of data jointly can be bundled within SyRI into a detailed image which drastically reveals the private life of the citizen.

5.58 The consequences of the processing of data for the data subject (article 6 section 4 sub c GDPR) can be considerable. The scale at and the intensity with which SyRI enables data processing results in a deep encroachment on privacy. Pursuant to article 5a.5 section 1 'Besluit SUWI', project participants and administrative bodies can be informed of risk notifications. These risk notifications can be requested by the public prosecutor and the police (article 65 section 3 sub b 'Wet SUWI'). In this manner, the application of SyRI can lead to the imposition of sanctions of an administrative and a criminal kind.

5.59 Of importance is furthermore that the data which is processed in the context of SyRI is generally not obtained with the consent of the data subject, but in the context of the implementation of public tasks. Citizens, therefore, cannot exercise any influence on the processing of their data in the context of SyRI by withholding or withdrawing their consent for this. Generally, *function creep* poses a major risk to citizens.

5.60 Finally, appropriate safeguards in the sense of article 6 section 4 sub e GDPR cannot be said to exist. Adequate oversight, for instance, has not been provided for (see marginal nos. 5.71 t/m 5.73).

5.61 In view of the preceding, data processing within SyRI takes place in violation of the principle of purpose limitation and compatible use.

5.62 To the extent the State would want to appeal to the exception stipulated in article 6 section 4 GDPR, on the basis of which deviations from the principle of compatible use are possible, it applies that the criteria for this have not been met. It can solely be appealed to in case of a legal provision which constitutes a necessary and proportionate measure in a democratic society to assure what is stipulated in the objectives listed in article 23 section 1 GDPR. As in case of SyRI there is not a situation of a necessary and proportionate measure, this exception cannot sustain the case for the State. In addition it applies that – even if the conditions for an appeal to the exception in article 6 section 4 GDPR were to be met – that this exception is in conflict with article 8 ECHR and so must be left unapplied.

Unlawful computerised individual decision-making

5.63 Article 22 section 1 GDPR contains a prohibition of the taking of decisions exclusively based on computerised processing, including profiling, which entail legal consequences

for the data subject or which otherwise impact him to a considerable degree (article 15 Rl and 42 Wbp). One must thereby be wary of the forming of semi-automatic decision-making, whereby a human decision may be involved, but the human component is subordinate to such an extent to, or dependent on, the computerised system, that computerised decision-making can in essence be said to pertain (**Productie 22**, p. 8). This is a real risk for risk profiling systems such as SyRI.[53] And the more invading the breach of one's private life, the more weight should be attributed to human intervention. 'Legal consequences' can be involved already in the event the data subject is subjected to increased surveillance measures (**Productie 22**, p. 10).

5.64 Within SyRI, the computerised processing of personal data takes place to evaluate, analyse, and predict personal aspects of citizens. Considering the broadly formulated categories of data which can be processed within SyRI, it regards quite varied aspects, such as 'professional performances', 'economic situation', 'reliability' and 'behaviour' as listed in article 4 sub 4 GDPR. Thereby, profiling in the sense of GDPR pertains. On this basis, it is decided with regard to individual citizens whether or not to issue a risk notification.

Non-compliance with information obligation

5.65 GDPR obliges every data controller to inform data subjects beforehand of the processing of their personal data. In case personal data is processed for another purpose than the one it was obtained for, such information must also be provided prior to the data processing. If the data subjects are not informed, they effectively lack the possibility of demanding the perusal, rectification, or removal of data or to exercise their rights regarding profiling. This is in conflict with the essence of the right to an effective judicial remedy.[54]

5.66 For the application of SyRI, the information obligation is not complied with. This is evinced by the documentation requested by Complainants. In the project Capelle, 137 notifications were inscribed in the register. Of those 137 persons, 0 have been informed (**Productie 17**, p. 4).

5.67 According to the government, it would require a 'disproportionate exertion' and it would open up 'the modus operandi' to which calculating citizens could adjust their behaviour.[55] This motivation does not suffice, however, to be able to make a valid appeal to the exception referred to. It is evinced, after all, by the ruling of the monitoring authority of AP regarding the data processing by SIOD, that exceptions to the information obligation must be applied in a restrictive manner. The State must weigh from case to case whether

[53] WRR Rapport, *Big Data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press 2016, p. 66.

[54] ECJ 6 October 2015, case C-362/14 (Schrems), r.o. 95.

[55] *Kamerstukken II*, 2012-2013, 33 579, no. 3, p. 23 ('Memorie van Toelichting').

and for how long an appeal to grounds for refusal is justified. A general appeal to a legal exception does not suffice (see marginal number 3.9).

5.68 The State must substantiate why the informing of citizens would entail such a disproportionate exertion. This has not come to pass. Furthermore, the government too swiftly reaches the conclusion that informing them is not possible at all. The information obligation can only be set aside 'in case and to the extent' grounds for exception pertain. To the extent the purposes of SyRI could, indeed, be impaired, the State must consider, therefore, to what extent the informing of data subjects is still possible without this issue manifesting itself. It could be decided, for example, to only inform data subjects at a later stage, after the processing of data in SyRI has been completed. This is also what was advised by the legal advisory body of 'Raad van State' (**Productie 11**, p. 8).

5.69 The position of the State that, by complying with the information obligation, it would reveal its modus operandi, has not been elucidated further either. How the informing of data subjects would be an obstacle to the application of SyRI does not become clear. That calculating citizens would be able to adjust their behaviour is improbable. After all, the processing of data in SyRI regards behaviour which has already taken place. But even if it were the case, the State must further weigh here as well what form of provision of information would, on the other hand, be possible.

5.70 Where it regards the application of profiling, the information to be provided to the data subjects must contain, amongst other things, 'useful information on the underlying rationale, as well as the interest and the expected consequences' (article 14 section 2 sub g GDPR). The State must, therefore, in any case indicate clearly what risk indicators were applied. After all, data subjects can only exercise their legal rights with regard to profiling, such as the filing of an objection, effectively if they know that such profiling is occurring.

Independent oversight not assured

5.71 The application of SyRI is not subject to any form of independent oversight. There is no judicial assessment, nor is there any assessment by another independent body. Oversight lies entirely with the responsible Department itself. Due to this omission, there is no controllable, adequate, and effective guarantee whatsoever against the abuse of SyRI, not beforehand and not afterwards. This, while the collaborating administrative bodies obtain a quite far-reaching freedom to determine the scope and set-up of SyRI-projects.

5.72 It is furthermore evinced by the Wob-documents that the assessment of the request by the Department does not consist of anything beyond a formality based on an unsubstantiated advice of LSI.[56] Objectionable in this context as well is that the risk models and

[56] GALOP II: Wob-document 4, can be found on https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 4/16; Afrikaanderwijk: Wob-document 28, can be found

indicators applied are kept secret and that it is not known what categories of personal data is processed in a concrete SyRI-project. It is of importance as well that the party which implements the linking of files and the data analysis – intelligence agency 'Inlichtingenbureau' – is not bound by a processor agreement. In a processor agreement, after all, arrangements must be stipulated with regard to the exercise of oversight by the Department in his capacity of data controller.

5.73 In view of the preceding, the application of SyRI is subject to a form of (independent) oversight which is compliant with the requirements which are established for it as evinced by the rulings of ECHR.

Lack of a processor agreement

5.74 In case of the processing of data in the context of SyRI, the Department acts as data controller and 'Inlichtingenbureau' as processor (article 5a.a. section 2 'Besluit SUWI'). On grounds of article 28 section 3 GDPR, between the Department and 'Inlichtingenbureau' a processor agreement should have been concluded. In his reply to the Wob-request of Complainants, the Department has indicated, however, that such processor agreement does not exist 'because "Inlichtingenbureau" has already been designated as processor in "Besluit SUW"' (**Productie 17**, p. 4). This remark derives from the faulty assumption that the conclusion of a processor agreement would not be required if an organisation has been designated as processor by law. In a processor agreement, after all, detailed arrangements must be made regarding the implementation of the processing of data. The safeguards which are normally established in a processor agreement, are laid down neither in 'Wet SUWI' nor in 'Besluit SUWI' with regard to 'Inlichtingenbureau'.

5.75 Due to the lack of a processor agreement, the State acts in violation of article 28 GDPR (article 14 Wbp) and thus unlawfully. This means that the processing of data by 'Inlichtingenbureau' has until today taken place unlawfully.

Violation of non-disclosure obligations

5.76 As explained, 'Wet SUWI' and 'Besluit SUWI' do not provide for a sufficient legal basis, in view of the requirements of article 8 ECHR, for the processing of personal data by way of SyRI. These legal arrangements thereby do not provide either for a legal basis for the breaching of the non-disclosure obligations in 'Wet SUWI', social benefits legislation 'Participatiewet', taxation law 'Awr' and administrative law 'Awb' (see marginal numbers 4.35).

---

through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file5/16; Capelle: Wob-document 46, can be found through https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri, file 6/16.

Conflict with article 6 ECHR

5.77 The Department can provide risk notifications which derive from a SyRI-project to administrative bodies and persons within the partnership (article 5a.3 section 2 'Besluit SyRI'). For these administrative bodies and persons, a risk notification can be grounds for the taking of administrative measures, such as the imposition of fines or the reclaiming, revoking of benefits, subsidies, or permits. The risk notification can also lead to civil, fiscal, or criminal proceedings. In all those cases, the information which is processed within SyRI can serve as evidence of the violation by the citizen of certain legal standards. As the deployment of SyRI can thus have an impact on the fairness of the proceedings at a later stage, thereto apply the safeguards of article 6 ECHR.

5.78 The legal arrangement, the use of SyRI, and the manner in which risk notifications are made in various ways result in a violation of article 6 ECHR. In the first place, no 'equality of arms' pertains. This principle implies that each party has a reasonable possibility of bringing his viewpoint to the fore and that they have access to the same information, under circumstances which do not bring him in a substantially more disadvantageous position than the other party. For citizens who in proceedings against the authorities are confronted with information from SyRI or with a risk notification, it is quite complicated, if not impossible, to contest or refute the correctness of a risk notification. They are not informed, after all, of the application of SyRI and in principle they are not granted the perusal of the information on which the risk notification is founded. Nor is it clear what risk models and indicators were applied.

5.79 In the second place, the presumption of innocence is violated. The acts of prosecution which flow from a risk notification can in individual cases create such a biased picture of the person involved that his/her guilt has already been established by the enforcing administrative bodies which must act upon the risk notification. It must thereby be taken into consideration that these parties assume that the risk notification derives from a neutral computer algorithm which makes use of objective, factual information and that on such basis a risk notification has come about. The Council of Europe in a recent report addresses the risks of the use of algorithms for the purpose of computerised systems which predict whether an individual may commit a violation:

> *'Such approaches may be highly prejudicial in terms of ethnic and racial backgrounds and therefore require scrupulous oversight and appropriate safeguards. Often the systems are based on existing police databases that intentionally or unintentionally reflect systemic biases. Depending on how crimes are recorded, which crimes are selected to be included within the analysis and which analytical tools are used, predictive algorithms may thus contribute to prejudicial decision-making and discriminatory outcomes.*
>
> *In addition, considerable concerns exist that the operation of such assessments in the context of crime prevention is likely to create echo chambers within which pre-*

existing prejudice may be further cemented. Bias or prejudice related, for example, to racial or ethnic background, may not be recognised as such by the police when integrated into an automated computer program that is deemed independent and neutral (see also 6.). As a result, bias may become standardised and may then be less likely to be identified and questioned as such. While it is unclear how prevalent such decisions created by algorithms are in the criminal justice system generally, the mere potential of their use raises serious concerns with regard to Article 6 of the ECHR and the principle of equality of arms and adversarial proceedings as established by the European Court of Human Rights.'[57]

6 DEFENCES

6.1 The Department of Social Affairs and Employment ('Minister van Sociale Zaken en Werkgelegenheid') has indicated on the occasion of consultations with the complainants that it does not agree with the objections of complainants (**Productie 20**). In the opinion of the Department, the requirement of foreseeability is complied with as it must be specified per project what data is required. This contention is incorrect because, as the government's advisory council 'Raad van State' has concluded as well, such assessment does not relieve the legislator from the obligation to describe the allocation of administrative powers and the associated limitation of fundamental rights as concretely as possible.

6.2 Furthermore, the Department has indicated as far as the informing of citizens is concerned that SyRI-projects are announced in various manners. In the first place, these projects are announced in the official gazette 'Staatscourant'. In addition, the mayor of Capelle aan den Ijssel has sent a letter regarding the SyRI-project. In Eindhoven, a flyer was used for this purpose. Finally, a citizen could file a request for perusal with the notification register. These circumstances do not eliminate the legal objections of complainants. After all, the Department persists in its contention that it is not obliged to inform individual citizens (**Productie 20**).

6.3 In conclusion, the Department contends that sufficient oversight has been provided, as the monitoring authority of 'Autoriteit Persoonsgegevens' can exercise oversight. This defence cannot resolve matters for the Department either. 'Autoriteit Persoonsgegevens' has liberty of policy in the deployment of its power of oversight and is not obligated, therefore, to exercise prior oversight on concrete projects whereby SyRI is deployed.

7 ADMISSIBILITY COMPLAINANTS

[57] Council of Europe, 'Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications', Committee of experts on internet intermediaries 2017, p. 11.

7.1 Complainants sub 1 to 3 defend a public interest pursuant to article 3:305a BW (Civil Code), which interest they defend each individually in accordance with their articles of association. The requirements of article 3:305a BW are complied with. Complainants are all an association or foundation, they defend the interests which are at stake in this matter, based on adequate descriptions of purpose in their articles and they all deploy activities in the field of the protection of fundamental rights, especially the right to privacy. Complainants have furthermore tried to achieve what is demanded in these proceeding by way of consultations. Complainants have requested the Department on 9 November 2017 for consultations. The attempt to achieve what is demanded in these proceedings through consultations has not produced any results.

7.2 The interests which Complainants stand up for furthermore are similar and are particularly suitable for bundling. Complainants defend various public interests, especially the interest of having respected fundamental rights and the interest of the protection of privacy. The interests defended by Complainants thereby exceed the interests of individual stakeholders.

7.3 Complainants sub 4 and 5 each individually have an interest in the legal action filed. As they have Dutch citizenship and are residents of the Netherlands, they make use of Dutch public facilities and therefore are constantly at risk of their personal data being processed within a SyRI-project.

8 COMPETENCE

8.1 The Court of Law of The Hague pursuant to article 99 Rv. (legal claims code) is competent to hear the dispute, as the State of the Netherlands has its seat in The Hague.

9 EVIDENCE

9.1 Complainants offer – without thereby assuming for themselves any onus of proof which does not legally fall to them – to prove the facts laid out in the present subpoena by all legal means, also including by way of experts' testimonies and the hearing of witnesses. Complainants reserve themselves the right to set out in detail the evidence in these proceedings.

9.2 The exhibits mentioned in this subpoena will be timely introduced into the lawsuit by Complainants.

THEREFORE:

That it may please the court to rule, as much as possible with immediate enforceability:

I. To declare that application of the articles 64 and 65 'Wet SUWI' and chapter 5a of 'Besluit SUWI' is incompatible with higher legislation, especially with article 8 ECHR, article 7 and 8 Charter and/or article 17 ICCPR; and/or article 6 and/or article 13 ECHR; and/or article 5, 6, 13, 14, 22 and/or 28 GDPR, or at least with the articles therewith corresponding from Wbp, or at least;

II. To declare that application of the following components of 'Wet SUWI' and 'Besluit SUWI' is incompatible with higher legislation, especially with article 8 ECHR, article 7 and 8 Charter and/or article 17 ICCPR; and/or article 6 and/or article 13 ECHR; and/or article 5, 6, 13, 14, 22 and/or 28 GDPR, or at least with the articles therewith corresponding from Wbp:

a) The description of purpose as included in article 64 section 1 'Wet SUWI'; and/or

b) The stipulation of powers for the processing of data and to deploy SyRI as laid down in article 64 section 3 and 64 section 4 'Wet SUWI'; and/or

c) The listing of categories of personal data as included in article 5a.1. section 3 'Besluit SUWI'; and/or

d) The practice of non-disclosure of risk models which are used upon deployment of SyRI; and/or

e) The arrangement with regard to the register risk notifications as included in article 5a.5 'Besluit SUWI'; and/or

f) The substantiation by the State of the necessity of SyRI; and/or

g) The arrangement whereby the individual administrative bodies are charged with the substantiation of the contention that the provision of data in the context of a SyRI project is proportional and commensurate, as stipulated in article 5a.1 section 4 'Besluit SUWI', and whereby an adequate, overarching assessment of those requirements was failed to be assured; and/or

h) The arrangement whereby data subjects are exclusively informed of the processing of their personal data in SyRI if it is the object of a risk notification and only upon request in such case, as stipulated in article 5a.5 'Besluit SUWI'; and/or

i) The arrangement for the oversight on the deployment of SRI, especially the fact that the Department 'Minister van Sociale Zaken en Werkgelegenheid' is the sole party which exercises supervision over the deployment of SyRI;

III. To declare that the processing of personal data which takes place in the context of, by way of and/or for the purpose of the deployment of, SyRI, especially the mutual exchange of personal data by administrative bodies (including the tax office 'de

Belastingdienst'), the provision of personal data to the Department (also including by 'de Belastingdienst'), the provision of personal data to the intelligence agency 'Inlichtingenbureau', the processing of personal data by 'Inlichtingenbureau', including profiling, the provision of personal data by 'Inlichtingenbureau' to the Department, the making of risk notifications and/or the inclusion of (information on) notifications in the notifications register, is unlawful on account of conflict with article 8 ECHR, article 7 and 8 Charter and/or article 17 ICCPR; and/or article 6 and/or article 13 ECHR; and/or article 5, 6, 13, 14, 22 and/or 28 GDPR and/or the articles corresponding therewith from Wbp;

IV. Articles 64 and 65 'Wet SUWI' and chapter 5a 'Besluit SUWI', or at least the components thereof as deemed incompatible by Your Court with higher legislation on grounds of demand I and/or II, or at least the components thereof as deemed incompatible as a principle of Justice by Your Court with higher legislation, be rendered ineffective or at least declared non-binding, or at least to establish that they must be left inapplicable, possibly by imposing such condition as may as a matter of Justice be established by Your Court of Law;

V. To declare that the State acts in violation of the non-disclosure obligations which the tax office 'de Belastingdienst' is subject to because 'de Belastingdienst' supplies personal data to other parties in partnerships on grounds of article 64 'Wet SUWI' and to the Department within the framework of SyRI;

VI. To order the State to render public the risk models and indicators which were used in the projects G.A.L.O.P. II and Capelle;

VII. To declare that the processing of personal data by the intelligence agency 'Inlichtingenbureau' is unlawful due to the lack of a processor agreement as intended in article 28 section 3 GDPR and/or article 14 section 2 Wbp;

VIII. To prohibit the State to process personal data, or at least the personal data of Complainants sub 6 and 7, in the context of, by way of and/or for the purpose of the deployment of, SyRI;

IX. To order the State to irreversibly destroy all personal data which was collected in the context of, by way of and/or for the purpose of the deployment of, SyRI, and to provide proof of such destruction to Complainants.

Condemning the defendant to bear the costs of these proceedings, increased by the statutory interest thereover as from 14 days after the date of the sentence to be pronounced in the present matter.

Bailiff

The costs of this writ for me, the bailiff, amount to € …...

This case is handled by:
Anton H. Ekker, & Douwe M. Linders

Deikwijs Advocaten
Panamalaan 8A
1019 AZ Amsterdam
T: +31 (0)20 2 614 614
F: +31 (0)20 2 614 615
www.deikwijs.nl - info@deikwijs.nl

EXHIBITS

Productie 1	Articles of association NJCM
Productie 2	Articles of association 'Platform Bescherming Burgerrechten'
Productie 3	Articles of association 'Privacy First'
Productie 4	Articles of association KDVP
Productie 5	House Regulation 'Landelijke Cliëntenraad'
Productie 6	Column Maxim Februari in 'NRC Handelsblad', 7 October 2014
Productie 7	Fragment lecture 'Kousbroeklezing' by Tommy Wieringa, 1 April 2015
Productie 8	CBP, 'Notitie Fraudebestrijding door Bestandskoppeling', 2006
Productie 9	CBP, findings internal report 'Bevindingen ambtshalve onderzoek Waterproof', 2007
Productie 10	Advice of legal council 'Raad van State' on the legislative proposal SyRI, 2012
Productie 11	Advice of 'Raad van State' on the concept decision SyRI, 2014
Productie 12	Advice of CBP on the legislative proposal SyRI, 2012
Productie 13	Advice of CBP on the concept decision SyRI, 2014
Productie 14	Article 64 and 65 'Wet SUWI'
Productie 15	Decree 'Besluit SUWI'
Productie 16	'Wob' (governance transparency) request of complainants of 12 December 2016
Productie 17	Partial ruling 1 in response to Wob-request of 8 March 2017
Productie 18	Partial ruling 2 in response to Wob-request of 6 June 2017
Productie 19	Partial ruling 3 in response to Wob-request of 5 July 2017
Productie 20	Report of consultations with the Department on 15 January 2018
Productie 21	Article 29-'Werkgroep Opinie doelbinding' (taskforce on purpose limitation), 2013
Productie 22	Article 29-Werkgroep Opinie profilering en geautomatiseerde besluitvorming (taskforce of profiling and computerised decision-making), 2018