UiO : Faculty of Law
University of Oslo

# One-stop-shop – or not?

The Regulation of competent supervisory authority in the new EU General Data Protection Regulation – does the one-stop-shop mechanism live up to its promise?

Candidate number: 8024

Submission deadline: 01.12.2016

Number of words: 17854

## Table of contents

# 1 Introduction

## 1.1 Introduction

The Court of Justice of the European Union (hereafter "the Court") has trough its interpretation of the Data Protection Directive (hereafter the Directive) extended the scope of EU data protection law in recent years. The most notable cases are Google Spain and Weltimmo.[1] The Court's willingness to interpret the Directive flexibly to ensure a high level of data privacy protection was a crucial element in both.[2]

As a result of the Court's approach, establishments not previously considered to be within the scope of EU data protection law, now have to comply with national rules pursuant to the Directive. In the wake of these judgements, some establishments have faced potentially significant administrative burdens having to deal with 28 EU supervisory authorities, three EEA supervisory authorities and a corresponding number of divergent national rules.

Concurrent with these developments in current law, the EU legislature enacted a new general data protection regulation (hereafter the Regulation).[3] One of the stated goals of the Regulation is to remove "[…] the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year".[4] Key to fulfilling this goal is the so-called one-stop-shop mechanism. This mechanism aims at ensuring that "[…] when the processing of personal data takes place in more than one member state, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions."[5]

The new Regulation also broadens the scope of EU data protection law, including undertakings not established, or using means of processing in the Union.

---

[1] Case C-131/12 (Google Spain SL and Google Inc. versus Agencia Española de Protección de Datos (AEPD) and Mario Costeja González) and Case C-230/14 (Weltimmo s. r. o. versus Nemzeti Adatvédelmi és Információszabadság Hatóság).

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The Regulation entered into force on 24 May 2016, but it shall not apply until 25 May 2018.

[4] Reform of EU data protection rules (2016)

[5] Data protection: Council supports "one-stop-shop"principle (2013)

## 1.2 **Topic and research questions**

Data protection law in EU has two paramount objectives:

- ensuring effective and complete protection of the right to privacy[6]; and
- removing the obstacles to flows of personal data, which might distort cross border competition.[7]

These goals are both continued and strengthened in the new Regulation. The Commission states the following about the goals of the reform:

> "The Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year." [8]

The former objective, strengthening citizens' fundamental rights, is achieved by inter alia extending the scope of the Regulation, and the latter is achieved by e.g. introducing the one-stop-shop mechanism.

In this thesis, I will critically assess two questions; the scope of EU data protection law, and the one-stop-shop mechanism.

Initially, I will compare the scope of EU data protection law in the Directive to the Regulation. The goal is to assess how the scope has changed – particularly in light of recent case law. My hypothesis is that the scope has extended, affecting undertakings not established or using means of processing in the Union.

Then, I will evaluate whether or not the one-stop-shop mechanism adopted in the Regulation will fulfil the promises of the EU legislature, and reduce administrative burdens, facilitate more efficient cross border flows of personal data and increase legal certainty for controllers, processors and supervisory authorities.

In summary, I will try to discern how the scope of EU data protection law has changed with the Regulation. Then I will discuss whether or not the one-stop-shop mechanism will live up to the promises heralding it.

Some readers might question why I have chosen to discuss the scope of EU data protection law and the one-stop-shop mechanism in one thesis with

---

[6] See for instance the Directive preamble 2 and 10 and Weltimmo para. 30.
[7] See inter alia the Directive preamble 7.
[8] Reform of EU data protection rules (2016)

limited space. In my view, there are good arguments for discussing these two topics together:

- Recent case law concerning the scope of the Directive treats different issues and topics that find parallels in the new Regulation. One example is the interpretation of the notion of establishment – which is thoroughly discussed in the Weltimmo case – and has direct relevance for the interpretation of "main establishment" in the Regulation is. The concept of "main establishment" is a key assessment for an evaluation of the one-stop-shop mechanism.
- Moreover, the case law on the scope of the Directive, namely Google Spain and Weltimmo, illustrate the Court's approach to EU data protection law, its principles of interpretation and how it assesses the different objectives and weighs them up against each other. I find ample guidance in case law and would be pressed to evaluate the one-stop-shop mechanism without the Court's reviews of these issues.

Based on this, I believe that a systematic review of the scope of the Directive – and also the scope of the Regulation – is a necessary foundation for a rigorous assessment of the questions concerning the one-stop-shop mechanism.

### 1.3 **Structure**

In chapter 2, I will highlight and explain the methods underpinning this thesis.

In chapter 3, I will compare the scope of the Directive with the Regulation, and assess how the scope of EU data protection law has changed, and discuss recent case law. The courts approach to Article 4 in the Directive is key to this assessment.

Further, in chapter 4, I will look at the political promises preluding the Regulation, creating a backdrop for my analysis of the mechanism as adopted. Following this, I will critically assess the new one shop stop mechanism and discuss the relationship between the general rule (the one-stop-shop mechanism) and the exceptions. The impact of the various exceptions is key to the overall evaluation of the mechanism.

Finally, in chapter 5, I will briefly summarize and conclude my thesis. My main findings are that the scope of EU data protection law has indeed been broadened, and that the one-stop-shop mechanism falls somewhat short of the promises made during the legislative process. As a general rule, the mechanism seems appropriate, but the many and varied exceptions reduces foreseeability and legal certainty for all actors involved.

### 1.4 Document purview

The Regulation aims at ensuring a greater degree of harmonization and reducing red tape and administrative burdens in various ways:

First, the EU legislature has chosen to regulate privacy trough a regulation, rather than a directive, which means that the latitude for national adaptations is relatively narrow.

Second, the Regulation envisages mechanisms to ensure cooperation and consistency between supervisory authorities in Chapter VII in the Regulation. The European Data Protection Board (hereafter the Board) and its competences is a related question.

Lastly, there are material changes – like removing the requirement to notify or seek approval from the relevant supervisory authority in many cases. I will not discuss these issues further due to space constraints.

While the Regulation will ensure a far greater degree of harmonisation than the current directive allows, there are exceptions, and a certain room for national adaptations.[9] In certain cases choice of law questions will therefore be key. I will not discuss this due to space constraints.

Furthermore, the Regulation, as the current directive, distinguishes between processing "in" the EU and outside of the EU.[10] Some scholars argue that the recent case law from the Court has blurred the lines between these two separately regulated questions by expanding the scope of European data protection law at least partially based on a "[…] lack of trust in the EU–US Safe Harbour scheme and other data transfer arrangements, fuelled by the Snowden revelations" and that this "[…] must have brought the CJEU to its 'flexible' and broad understanding of the scope of Article 4(1)a of the Data Protection Directive due to a perceived lack of alternative in terms of effective fundamental rights protection".[11] One could therefore reasonably expect that the question of transfers would be part of this thesis. Due to space constraints, I will however not discuss this issue.

## 2 Methods

### 2.1 Interpretation of EU law

No provision in the treaties of the European Union[12] explicitly regulates the interpretation of EU law. Case law from the Court of Justice of the Europe-

[9] See for instance the Regulation Articles 6(2), 8(1), 9(4), 23, and 85.
[10] The Regulation governs transfers of personal data to third countries or international organisations in Chapter V, the Directive governs similar questions in its Chapter IV.
[11] de Hert and Czerniawski (2016) page 6.
[12] Treaty on European union (Consolidated version 2016) - OJ C 202 (2016) Treaty on the Functioning of the European Union (Consolidated version 2016) - OJ C 202 (2016) Charter

an Union (hereafter the Court) has however given considerable methodological guidance both explicitly (in cases like the CILFIT-case discussed below), and implicitly through its continued practice.

I find that the CILFIT-case illustrates the court's interpretative practice elegantly, and discusses its main points in the following.[13]

The Court starts off underlining the importance of looking at the different language versions when interpreting community law. Nuances or differences in meaning, might give indications as to what the EU legislators meant when enacting the relevant provision.

Moreover, the Court emphasises the need to assess whether or not the terminology used is particular for Community law, and if so what meaning the terminology has in an EU law context. There are various examples of this, for instance the meaning of the word "undertaking". In a state-aid-law context for instance, the meaning may be different from everyday speech.

Finally, the Court stresses the necessity of interpreting the relevant provisions in light of their context, in view of community law as a whole, and keeping in mind the stated objectives of the legislation – interpreting the law teleologically.

I will also – as stated above – look at relevant case law for guidance, and look at principles of interpretation recurring in case law. This is naturally primarily relevant for the Directive, but when the the wording of provisions is continued in the Regulation, or aims, objectives or concepts are similar, I will also lean on case law for guidance for the Regulation. For the Regulation, the primary and most important source of law will be the Regulation itself, and while preparatory works has far less weight in EU law than they have in for instance Norwegian legal tradition, preparatory works, comparing final versions to earlier drafts of the legislation and similar sources will be necessary to shed light on ambiguously worded provisions.

A source of law that is unique for the area of EU data protection law, is opinions from A29WP.[14] These are not legally binding, and as such have limited formal importance compared to other sources of law. On the other hand, they are indicative of the consensus on current law among European supervisory authorities. And they are therefore by their very nature a source that will shed light on both current and future authority practice. So

---

of Fundamental Rights of the European Union (2016) - OJ C 202 (2016) Treaty of Lisbon (2007) - OJ C 306 (2007).

[13] Case 283/81 (CILFIT) para. 18-20.

[14] Working Party on the Protection of Individuals with regard to the Processing of Personal Data pursuant to Article 29 in the Directive.

while their legal weight, as a general rule, is low, their practical weight is considerable.

Weighting these various interpretative factors to discern the correct interpretation will necessarily be a discretionary exercise. The balance between them will depend on the relationship between the factors and the factors themselves. An unambiguously worded provision or an unequivocal Court case will unavoidably carry great weight. Some scholars state that "where the wording of an EU law provision is clear and precise, its contextual or teleological interpretation may not call into question the literal meaning of that provision, as this would run counter to the principle of legal certainty and to the principle of inter-institutional balance enshrined in Article 13(2) TEU. Stated simply, the ECJ will never ignore the clear and precise wording of an EU law provision". [15] Conversely, a more ambiguous provision may necessitate ascribing the stated objectives of the legislation or preparatory documents more weight.

### 2.2 **Interpreting other sources**

I also discuss and assess policy statements and other various statements from the EU legislature, in an effort to create a snapshot of how the one-stop-shop mechanism was touted by lawmakers before the Regulation was adopted.

These sources vary greatly in both formality and prominence, from press releases from the various involved actors, to various drafts and position statements part of the official legislative process. As a starting point I will emphasize the more formal documents more. At the same time, for those undertakings following the process, not familiar with the intricacies of the EU legislature, the press releases and various public statements are probably what they have perceived as the key message – and what they have acted in reliance on.

## 3 Territorial scope

### 3.1 **Introduction**

The main goal of this chapter is to discern whether the Regulation extends the scope of EU data protection law. To do so I must ascertain the scope of both the Directive and the Regulation.

First, I will elaborate on Article 4 in the current directive, delineating the scope of the Directive. Then, I will critically assess and interpret Article 3 in the GDPR with the same goal: to determine the scope of the Regulation. Finally, I will compare the scope of the Directive with the Regulation and briefly discuss whether my hypothesis – that the scope has been extended – is correct.

[15] Lenaerts, Gutiérrez-Fons (2013) page 7.

## 3.2 **Article 4 in the Directive – National law applicable**

### 3.2.1 Introduction

The Directive treats the issue of scope in Article 4 on national law applicable. The Court has applied a flexible interpretation of this article on to ensure a high level of protection for data subjects in the Union. In this subchapter, I will provide further detail on the decisions driving this development and discuss Article 4 in general.

I will discuss the interpretation Article 4 in the following, placing particular emphasis on Google Spain and Weltimmo.[16]

In Google Spain, the main question with relevance to this thesis was whether the Directive applied to processing operations outside the Union if the undertaking had a branch in a Member State. The Court found that the link between the Spanish branch of Google and the establishment in US was of such a nature that EU law applied.

In Weltimmo, the case concerned the question of competent supervisory authority and the question of applicable law. For this thesis, the discussion on the meaning of "establishment" in the context of the Directive is most relevant. The Court concluded that since Weltimmo had – by way of a one-man operation – "real and effective activity […] exercised through stable arrangements" in Hungary, it was established in that jurisdiction.

Article 4 in the Directive mandates that national laws should apply when the processing is "[…] carried out in the context of the activities of an establishment of the controller on the territory of the Member State". Furthermore, the Directive mandates the application of Member State law when a controller is not established on Community territory, but "[…] for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community".[17]

The legal starting point is therefore that the rules in the Directive apply in two main processing situations – both linking scope to Union territory:

- processing in the context of an establishment in a Member States; and

[16] Case C-131/12 (Google Spain) and Case C-230/14 (Weltimmo).

[17] In addition, the Directive applies to processing of personal data where national law applies by virtue of international public law. This is of scant relevance for this thesis, and will therefore not be discussed further.

- processing using equipment (or means) on the territory of a Member state.

It is not, however, easy to demarcate the scope of the Directive based on the wording of Article 4 alone. The provision raises several questions:

- What constitutes an "establishment"?
- What does "[…] in the context of the activities of an establishment […]" mean?
- How should the phrase "for purposes of processing personal data makes use of equipment" be interpreted?
-

### 3.2.2 Establishment

I will discuss the concept of establishment first. The Directive has, as mentioned above, a two-pronged approach to scope. It distinguishes between controllers established in the Union, and those not established in the Union. It is therefore necessary to clarify what "establishment" means.

The preamble gives some guidance on this question. Recital 18 states that establishment "[…] implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect". The wording implies that activity and stability takes precedence over the legal form of such an establishment.

The Court expanded on this in Weltimmo, where it clarified the criteria for considering an arrangement an "establishment" in more detail. The activity in question consisted of one single person which the Court found to constitute an establishment.[18]

The Court stated that a "flexible definition of the concept of 'establishment'" is necessary to avoid circumvention of national rules.[19] The Court held that even a single representative – if it acts with a sufficient degree of stability trough the presence of the necessary equipment – is sufficient to meet the "establishment" criteria. The Court emphasized this by stating that the concept of "establishment" in the Directive "[…] extends to any real and effective activity — even a minimal one — exercised through stable arrangements".[20] The Court gave the purpose of the Directive decisive weight in its interpretation.

Some scholars describe this teleological approach as such: "[…] legal provisions are not necessarily read literally but are understood in the light of the purpose, values, legal, social, and economic goals these provisions aim to

[18] Case C-230/14 (Weltimmo), inter alia para. 30-31.
[19] Case C-131/12 (Google Spain).
[20] Ibid, para 31.

achieve".[21] This is a precise description of the Court's methodology; Both Weltimmo and Google Spain show that the court is willing to interpret the relevant provisions broadly, if it is necessary to ensure a high level of protection for data subjects – a key objective in the legislation in question.

In conclusion, the "establishment"-requirement does not entail a very strict test for size, nor does it stipulate concrete formal or organisational requirements concerning corporate structure or legal form. The Court does however consider two factors crucial:

- real activity, and that the necessary processing equipment for that activity was present; and
- stable activities over some time.[22]

This is in line with earlier case law on the notion of establishment.[23]

### 3.2.3 Defining "in the context of the activities of an establishment"

The second question that has come to a head in case law is the meaning of the phrase "in the context of the activities of an establishment".

The Google Spain-case partially hinged on the question of whether the processing of Google's US based undertaking where "in the context of the activities" of Google's Spanish undertaking.[24] The activities of the latter were indented to promote advertising space offered by the search engine run by the former.

The Court emphasized the main objective of the Directive: the complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy. The Court also underlined the need for a flexible interpretation of the relevant provisions to ensure the attainment of this objective, and explicitly stated that the provision could not be interpreted restrictively. Furthermore, the Court pointed at the intention of the European Union legislature, namely "to prevent individuals from being deprived of the protection guaranteed by the Directive and that protection from being circumvented"[25].

The Court held that the advertising activities meant that the processing of Google's US based undertaking were in the context of activities of an establishment on Community territory.

---

[21] de Hert and Czerniawski (2016) page 5.
[22] Case C-230/14 (Weltimmo).
[23] See for instance the cases referred to in Opinion 8/2010 on applicable law (2010) page 11.
[24] Case C-131/12 (Google Spain).
[25] Case C-131/12 (Google Spain).

The crucial point in this case is how the Court evaluates the relationship between the Spanish and the American establishments. The Court uses the phrase "inextricably linked"[26] to describe the economic relationship between them. Moreover, the Court underlines the importance of the advertisement sales for the search engine and vice versa. The fact that the two parties involved have an interdependent relationship seems to be decisive for the outcome. In my view, the Court draws a line in the sand here. A line, which might indicate that there must be a substantial link between undertakings – both organizationally and economically – before processing, is deemed to be in the context of the activities of an establishment.

On this topic, the WP29 states that"[i]t would be a mistake to read the CJEU ruling too broadly, and conclude that any and all establishments with the remotest link to the data processing activities will trigger application of EU law. [...]"[27] They furthermore point at the fact that the income generated by Google Spain SL are not automatically used to fund European establishments, and state that "[...] the necessary economic link between the activities of the local establishment and the data processing activities may not have to be particularly direct to meet the criteria"[28] This indicates that while the Court most likely would not accept any remote link, one should not apply a too strict test on this point.

Some scholars seem to suggest that one cannot necessarily apply he lessons from Google Spain to cases not concerning search engines, I respectfully disagree – the main principal statements in the case aren't inseparably related to specific technologies or industries, and I believe that they are applicable also on other industries.[29] The WP29 seems to hold the same view, stating that "[i]t would be equally wrong to read the judgement too restrictively, and merely to apply it to the specific business model of search engine operators".

In my opinion, there are two main points to take from this case:

- the court is willing to interpreting provisions flexibly to ensure that the objectives of the Directive are achieved; but
- the Court still requires a substantial link between Union territory and the processing activities taking place.

[26] Ibid, para. 56.
[27] Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain (2015) page 5.
[28] Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain (2015) page 5.
[29] See inter alia Svantesson (2016) page 215

### 3.2.4 The meaning of "for purposes of processing personal data makes use of equipment"

The last of the important questions concerning the scope of the Directive, is how to interpret "for purposes of processing personal data makes use of equipment". This question has not come to a head in case law (and most likely will not, since the issue is moot from 2018 and forward).

As for the phrase "for purposes of processing personal data makes use of", the WP29 states that this indicate "some kind of activity of the controller and the clear intention of the controller to process personal data […] not necessary for the controller to exercise ownership or full control over such equipment for the processing to fall within the scope of the Directive".[30] I agree with this assessment, the wording of the provision does not imply ownership, nor full control – merely the possibility to use the equipment in question for said purposes.

The interpretation of the last word – "equipment" – illustrates the necessity of looking at the various language versions of EU legal texts. The Danish version uses the word "midler", and the German version "Mittel", both with a broader meaning than the English "equipment". The Swedish language version on the other hand, is closer to the English version, using "utrustning", which similarly to equipment has a more specific and narrow meaning.

When such ambiguousness arises, the relevant provision must be interpreted teleologically. In this case, the objective of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons is best served by choosing the broader "means" over "equipment". The Court also emphasises that the European Union legislature has prescribed a particularly broad territorial scope for the Directive, precisely to ensure a high level of protection and to avoid circumvention. It is also worth pointing to the fact that the English language version also uses the word "means" in the preamble.[31]

Bygrave states that "[t]he reference to "equipment" gives an impression that something materially substantial and solid must be used. Such an impression, however, is somewhat misleading. Recital 20 in the preamble to the Directive mentions simply "means used"; i.e. it drops the more technical term "equipment". Other language versions of the Directive tend to refer simply to "means" (French "moyens"; German "Mittel"). In other words, the term is to be construed broadly and somewhat loosely", mirroring my assessment above.[32]

---

[30] Opinion 8/2010 on applicable law (2010) page 20.
[31] The Directive, preamble 20.
[32] Bygrave (2000) page 7

Finally, also WP29[33] "[u]nderstands the word "equipment" as "means" […]".[34]

Overall, I have reached the conclusion that the wider meaning of "means", "midler" or "Mittel" must be favoured over a narrower interpretation of the word "equipment". From this one can assume that the provision does not necessarily require physical apparatuses or equipment in the Union to apply, meaning that e.g. virtual servers or software used in a Member State may be enough to be covered.

### 3.2.5 Summary

Resent case law has given us a somewhat clearer view of the scope of the Directive. The main take away from recent cases is that the Court is very aware of the need for a flexible and non-restrictive interpretation of the relevant provisions.

As previously mentioned, some scholars believe that this has been brought on by "[…] the lack of trust in the EU–US Safe Harbour scheme and other data transfer arrangements, fuelled by the Snowden revelations […]" and that this "[…] must have brought the CJEU to its 'flexible' and broad understanding of the scope of Article 4(1)a of the Data Protection Directive due to a perceived lack of alternative in terms of effective fundamental rights protection".[35] This is a plausible and compelling explanation, but it is very hard to substantiate or verify.

Regardless of the motivation of the Court, the objective of ensuring effective and complete protection of the right to privacy has taken centre stage in privacy cases before the Court. It also seems clear that the Court is willing to apply a flexible interpretation of the law to safeguard that objective. At the same time, the Court has not abandoned the territoriality principle completely. The Court still demands some connection between the processing taking place, and Union territory. [36]

It is worth noting that pursuant to the Directive, competence of a supervisory authority and applicable law are two separate questions. In Weltimmo, the Court states that "[…] Article 28 of Directive 95/46, entitled 'Supervisory authority', deals with the role and powers of that authority. […] The national law applicable to the controller in respect of that processing must therefore be determined not in the light of Article 28 of Directive 95/46, but in the light of Article 4 of that directive".[37] Furthermore, that a "supervisory authority […] may examine [a] complaint irrespective of the applicable

[33] Working Party on the Protection of Individuals with regard to the Processing of Personal Data pursuant to Article 29 in the Directive.
[34] WP29 Opinion 8/2010 on applicable law, page 20.
[35] de Hert and Czerniawski (2016) page 6.
[36] Ibid page 5.
[37] Case C-230/14 (Weltimmo) para. 23.

law, and, consequently, even if the law applicable to the processing of the data concerned is that of another Member State".[38]

## 3.3 **Article 3 in the Regulation – territorial scope**

### 3.3.1 Introduction

In this subchapter, I will assess the scope of the new Regulation, and compare it with the Directive.

In the new Regulation, the scope of the legislation is covered in Article 3. The Regulation applies in two main situations:

- processing in the context of an establishment in a Member States, and
- processing where an establishment outside the Union targets data subjects in the Union.[39]

The first situation, processing in the context of an establishment in a Member State is textually very similar to the current provision in the Directive. The second situation, targeting data subjects in the union, is new. This unequivocally severs the link between EU data protection law and the Union territory.

### 3.3.2 Defining "processing of personal data in the context of the activities of an establishment"

The wording of the first section is very similar to the corresponding provision in the Directive. There are however some differences. First, as discussed above, the Regulation governs Union territorial scope, while the Directive governs Member State territorial scope.

Second, the Regulation references processing of personal data in the context of the activities of an establishment of the controller or the processor, while the Directive only references the controller.

There is no evidence that the EU legislature intended to imbue a different meaning in the words "in the context of the activities of an establishment" in the Regulation compared to the Directive. On the contrary, the choice of near identical wording implies that the EU legislature meant to continue the content of the provision. That furthermore means that the existing case law inter alia the Google Spain and Weltimmo cases, is still relevant for the understanding of the Regulation.[40]

---

[38] Ibid para. 54.

[39] In addition, the Regulation applies to processing of personal data where national law applies by virtue of international public law. This is of limited relevance for this thesis, and will therefore not be discussed further.

[40] Case C-131/12 (Google Spain), and Case C-230/14 (Weltimmo).

One can also assume that the EU legislature consciously chose to include the new phrase "[…] or a processor […]" to serve a certain purpose and to change the status quo. This may widen the territorial scope in situations where an establishment of the processor (and not the controller) have activities in EU, and those activities can be inextricably linked to the processing of personal data outside the Union. The arrangements that will be covered by this, is not immediately evident. The change may serve to counteract creative corporate arrangements, and furthermore signifies the EU legislatures continued goal of a broad territorial scope to avoid circumvention of the rule. Furthermore, it ties neatly into the legislature's aim of assigning more responsibility directly to data processors, and as such strengthens the Regulations internal consistency.

I refer to the discussion above in para 3.2.3 for a more detailed discussion on the parts of the provision that are mirrored by the corresponding provision in the Directive.

### 3.3.3 Controllers or processors not established in the Union

The next question is how the Regulation governs controllers or processors not established in the Union. The Regulation applies to the processing of personal data of data subjects who are in the Union, by a controller or a processor not in the Union if the processing activities are related to the:

- offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or
- monitoring of the behaviour of data subjects who are in the Union as far as their behaviour takes place within the Union.

This severs the link between the scope of EU data protection law and Union territory.

The wording of these provisions raises several questions:

- What does the phrase "in the Union" mean?
- What is required to consider goods or services offered **to** data subjects in the Union?
- How should one understand the term "monitoring of behaviour"?

### 3.3.4 "Data subjects in the Union"

A common criterion in both alternatives is the requirement that the data subject must be "in the Union". In the 2012 draft of the Regulation, Article 3(2) stated that Regulation applies for "[d]ata subjects **residing in** the Union [...]"[41]. In the adopted version, the corresponding wording is that "[d]ata subjects who are **in** the Union" (my emphasis both places).[42] A textual in-

[41] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft (including explanatory memorandum) Article 3(2).
[42] The Regulation Article 3(2).

terpretation implies that "in" must be interpreted to mean something less formal, and more extensive than "residing in", the latter entailing associations to permanency and formal requirements. The European Parliament Committee on Industry, Research and Energy suggested using the phrase "domiciled in", in their opinion from early 2013.[43] Looking at preamble 14 in the Regulation, which states that "[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence […], it is clear that the EU legislature has moved away from requiring residency or domicile.

In conclusion, the provision entails that the scope of the Regulation covers all natural persons physically present in the Union, regardless of nationality and whether their stay is transitory or permanent.

### 3.3.5 "Offering goods or services to data subjects in the Union"

The next phrase which must be interpreted, is "offering goods or services to data subjects in the Union" by controllers or processors not established in the Union.

The wording of both the provision itself and preamble 23, clearly state that the provision applies irrespective of payment. This means that inter alia social media services, where the transaction between the user and the services more often than not take shape of exchanging a service for personal information/data, are covered.[44]

Furthermore, the phrase "goods or services" in Article 3 appears to be a very broad standard for applying the Regulation.

The expression "to data subjects" in Article 3 is more restrictive. In preamble 23, the legislators state that it must be "ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union"[45]

As for how to ascertain this, the preamble points to factors such as "the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union".[46] In my opinion, other factors like marketing in one or

[43] Opinion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (2012) page 46
[44] See for instance Spiekermann, Acquisti, Böhme, Hu (2015) page 161.
[45] Ibid.
[46] Ibid.

more member states, having an establishment in one or more member states, a free customer service phone number in one or more member states and other similar factors may also indicate the intention of the provider to provide goods or services to a Member State.[47]

The use of the word "envisages" indicates that the EU legislators want to differentiate between providers that are merely accessible from the Union, and providers that actively seek to attract customers form the Union. The wording of the provision imposes as a condition that the targeting is intentional.

This strikes a fair balance between the protection of the data subjects in the Union, and the legal certainty of undertakings. Undertakings will not be covered by merely being accessible for Union customers due to the global nature of the Internet. Without this condition, undertakings with no intention of offering goods or services to data subjects in the Union in particular would be covered by the territorial scope of the Regulation – a solution that would be a prime example of regulatory overreach.

The Court has discussed similar question in the context of other legislation. Inter alia in the joined cases C-585/08 and C-144/09, where the court discusses "[…]what criteria a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile"[48].

While the Court interprets the relevant provisions in light of their consumer protection objectives. I believe the similarity of the objectives and the wording of the relevant provisions permit an analogous application of the case. This is underlined by the Court stating that it must be determined whether "[…] there was evidence demonstrating that the trader was **envisaging** doing business with consumers […]" (my emphasis). [49]

Substantively, the Court states that the "[…] trader must have manifested its intention to establish commercial relations with consumers from one or more other Member States, including that of the consumer's domicile".[50]

Furthermore, the Court points at various evidence that might establish such an intention:

- mention of offering its services or goods in one or more member states;

---

[47] See comparably, HR-2010-01734-A para 31-33, where the Norwegian Supreme Court discusses analogous issues.
[48] Joined cases C-585/08 and C-144/09 (Peter Pammer (C-585/08), Hotel Alpenhof GesmbH (C-144/09) versus Reederei Karl Schlüter GmbH & Co KG (C-585/08), Oliver Heller (C-144/09)) para. 47.
[49] Ibid, para 76.
[50] Ibid, para 75.

- use of internet referencing services;
- the existence of activities directed to the relevant member state;
- mention of telephone numbers with the international code;
- the use of neutral (or different) top level domain as .com or .eu; and
- the mention of an international clientele, namely by reviews from such customers.[51]

This is not an exhaustive list, and it is naturally linked to the subject matter and the legislative context of this particular case. Even so, it is plausible that the Court would rely on similar factors when interpreting the Regulation.

As a conclusion, the assessment of whether an offer targeting entities in the Union must necessarily be highly discretionary, and based on the facts in each case.

#### 3.3.6 *Monitoring*

As for the word "monitoring", preamble 24 points at tracking of users, profiling, analysis and prediction of personal preferences, behaviours and attitudes. This implies a rather broad definition of the term. When this is prefaced by the word "related", the wording of the provision taken together implies a wide scope of application. Some scholars consider that "[…] data mining and data correlating methods enabling the evaluation, analysis, or forecasting of any parameter of the economic, social, and working life of an individual; as well as of any aspect of his personality (interests, preferences, etc.) may be caught by this definition of "profiling" […]".[52]

Preamble 24 of the Regulation describes tracking people on "the internet". In light of the objectives of the Regulation, the word "internet" should most likely not be interpreted to mean the Internet (capital I) only. Tracking of persons on local networks or other technologies than the Internet should be covered if the aims of the Regulation are to be achieved. Examples of this may be RFID-tracking of customer behaviour, NFC-tracking etc. This is supported by preamble 15, where it is stated that "[i]n order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used". Moreover, preamble 30 explicitly state that "[n]atural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags". As a final note, it is worth mentioning that the mere "potential subsequent use" of the data is sufficient, also increasing the scope of the provision.

[51] Ibid, para 80-83.
[52] Skouma and Léonard (2015) page 37.

### 3.4 **Summary**

Article 3(1) in the Regulation and Article 4(1)(a) in the Directive are fairly similar. Both provisions apply to processing in the context of the activities of an establishment in a member state or the Union. The most obvious difference is the inclusion of processors in the Regulation.

The Regulation departs more substantially from the Directive on processing of personal data of data subjects in the Union by controllers and processors outside the Union. The Directive requires on the use of means or equipment in the Union. The Regulation goes in a different direction with a two pronged approach:

The first alternative concerns processing activities related to the offering of goods or services to data subjects in the Union. As discussed above, this criterion requires that there is a deliberate targeting of customers in the Union. I find that this increases the predictability for undertakings. They can choose not to direct their offerings to customers in the Union[53] – and so avoid being within the territorial scope of the Regulation.

In my view, this strikes a proportionate (and necessary) balance between the interests of establishments outside the Union, and consumers in the Union. The alternatives – either excluding controllers and processors outside the Union altogether, or including all establishments having customers in the Union, are both too far reaching.

The former, excluding controllers and processors outside the Union, would to a great degree undermine the new Regulation, and make circumvention easy. The latter would be an aggressive jurisdictional overreach, and would affect establishments that not only are not familiar with the Regulation, but who has never intended to reach data subjects in the Union.

The second alternative concerns the monitoring of the behaviour of data subjects within the Union. Again, the provision links the scope to the intent of the establishments potentially covered by it. If they actively target data subjects in the Union, they are covered by the Regulation. At the same time, the territorial scope is demarcated for behaviour outside the Union, the opposite would have lead to jurisdictional overreach – effectively giving the Regulation effect for all monitoring of all data subjects globally. It is worth noting that some scholars disagree with this approach, stating for instance that this is an example of "[…] extreme extraterritoriality […]".[54] I on the other hand find that this approach strikes a reasonable balance, empowering undertakings outside the Union to choose whether they want to target

[53] This could be done passively, by not marketing in the Union, not offering Member State currencies, not having support in Member State languages etc., or actively by geoblocking or similar tools.

[54] Svantesson (2016) page 216.

Union subjects or not, and at the same time ensuring a high level of protection for data subjects in the Union. Some scholars believe that the new scope of EU Data protection law will potentially "[...] mean that many US companies targeting the EU market will be caught".[55] I agree with this assessment, but believe it to be necessary to ensure the needed protection for data subjects in the Union.

One core element to note from this chapter is that the Court has paid particular attention to the objectives of the Directive when interpreting the various provisions concerning territorial scope. It is highly likely that this will continue with the new Regulation.

The conclusion on this point is that the scope of EU data protection law has broadened. We have gone from a scope linked to territory, to a scope that also covers undertakings with no establishment, equipment or means for processing on the territory of the Union. Unequivocally severing the link to the territory is a bold move, but one I believe to be necessary to achieve the objectives of the Regulation, namely to ensure a high level of protection for persons in the Union and avoid circumvention.

A tangential issue – not directly relevant to my thesis, but nevertheless worth a brief mention – is the question of practical and real enforcement of the Regulation outside Union territory. While – as an example – the Finnish supervisory authority might find that they are legally competent to apply the Regulation to a Chinese undertaking providing services or goods to Finnish customers, it might prove difficult to enforce potential decisions. Some scholars has discussed this issue, underlining the "[…] greater difficulty in enforcing the law in a global context" and called for "[…] taking enforceability into account as a criterion for applying data protection law […]" because it could "[…] help deal with the growing number of legal conflicts involving regulation of international data transfers.[56]

# 4 The one-stop-shop mechanism

I have chosen to discuss two hypothesises in this thesis:

In the previous chapter, I compare the scope of EU data protection law in the new Regulation to the current directive. My findings are that the scope has indeed increased. The scope of the Regulation now covers undertakings without establishments in the Union – and not using equipment or means for processing in the Union (granted that they target data subjects in the Union). The concerned controllers and processors will have to ensure compliance with EU data privacy rules, leading to increased administrative costs.

[55] Burri and Schär (2016) page 21.
[56] Kuner (2015) page 236.

My second hypothesis is that the one-stop-shop mechanism fails to fulfil its potential. I will start this chapter by outlining the promises of the EU legislature in the time before the Regulation was adopted. I will base this assessment on various formal and informal sources like working papers and press releases.

Then I will assess whether or not the actual adopted Regulation lives up to the build-up by the EU legislature. I will do so by critically evaluating the division of labour, competences and responsibilities between the various supervisory authorities concerned in the Regulation.

My conclusion is that the one-stop-shop mechanism does not fully live up to the heralded reduction in red tape and administrative costs indicated by various sources before its adoption. The exceptions are too many and varied, and it therefore fails to create the legal certainty and predictability necessary for it to fulfil its promise.

## 4.1 The one-stop-shop mechanism as it was envisaged by the EU legislature before the Regulation was enacted

In this subchapter, I will discuss the general policy objectives of the Regulation. Then I will interpret various sources and delineate and more concretely define the one-stop-shop mechanism – as the EU legislators envisaged it before they finally adopted it. The aim of the exercise is to ascertain what it was reasonable for outsiders to expect during the proceedings.

The sources used in this chapter differ substantially in the degree of formality, from press releases on the one hand, to official reports on the other hand. While neither are legally binding documents or official sources of law, it stands to reason that one should place most emphasis on the more formal documents, and conversely place less emphasis on the more informal sources.

Looking at EU press releases and communications, "[…] enhanc[ing] the cost efficiency of the data protection rules for international business, thus contributing to the growth of the digital economy […]"was an important part of the motivation behind the reform of EU Data protection rules.[57] Moreover, the aim was to "[…] simplify the regulatory environment by drastically cutting red tape and doing away with formalities […]".[58]

[57] Data Protection: Council Supports "One-Stop-Shop"Principle, 2013.
[58] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st Century, 2012

The Commission highlighted "[…] reducing fragmentation, strengthening consistency and simplifying the regulatory environment, thus eliminating unnecessary costs and reducing administrative burden" as one of the three main policy objectives of the Regulation.[59]

When the Commission described the issues with the current directive , they underlined that it "[…] hamper[s] the functioning of the internal market and cooperation between public authorities in relation to EU policies"[60]

The Council of the European Union pointed to the one-stop-shop mechanism as one of two "[…] central pillars of the Commission proposal […]"(the consistency mechanism being the other), and that it would "[…] ensure consistent application, provide legal certainty and reduce administrative burden […]" for the concerned controllers and processors.[61]

These sources all seem to point at similar issues concerning the current directive:

- too much red tape;
- legal uncertainty;
- too heavy administrative burdens;
- unnecessary costs; and
- too much regulatory fragmentation.

Based on these sources the Regulation was meant to prevent these issues by introducing concepts as the consistency mechanism, the one-stop-shop mechanism and essentially removing the notification requirement.

In the preamble of the 2012 draft, the tasks and powers of the lead supervisory authority (hereafter LSA) is described as such: "one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors".[62] This statement clearly indicate that controllers and processors was envisaged to only deal with "one single" authority, and that this authority was supposed to be competent to take all related decisions.

Similarly the phrase "[…] data controllers in the EU will only have to deal with a single DPA, namely the DPA of the Member State where the compa-

[59] Commission Staff Working Paper Executive Summary Of The Impact Assessment (2012) Page 4
[60] Commission Staff Working Paper Impact Assessment (2012) Page 11.
[61] Data Protection: Council Supports "One-Stop-Shop"Principle.
[62] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (2012) Preamble 97.

ny's main establishment is located"[63] strongly indicates that cross border controllers and processors would not have to deal with a variety of national supervisory authorities, but only with the LSA pursuant to the one-stop-shop mechanism – regardless of the scope of the actual case.[64]

The Commission further describes the one-stop-shop mechanism as a system with a "[…] single law and one single DPA responsible […]".[65] One cannot reasonably interpret this to mean that the LSA only has the competence to act in certain types of cases, or in some specific stages of an investigation. On the contrary, this seems to imply that the LSA has a multitude of tasks and powers to ensure that the cross border processing of controllers and processors is subject to the scrutiny of only "one single DPA".

The available sources on envisaged one-stop-shop mechanism strongly imply that there was not meant to be any – or at least not many – exceptions to the one-stop-shop. These sources paint a picture of a one-stop-shop mechanism ensuring that the LSA is inter alia responsible for carrying out investigations, communicate with the controller or processor concerning possible infringements, monitor the application of the Regulation handle the controller/processor side of complaints, and taking the related decisions.

And while these are informal sources are not binding, they have shaped the expectations of controllers and processors both within and outside of the Union, and some have probably acting in accordance this and adapted their operations.

### 4.2 **The one-stop-shop mechanism – as it is**

In this subchapter, I will discuss the one-stop-shop mechanism as adopted in the Regulation.

I will start with looking at the general rule. Then I will review the main exceptions. Moreover, I will present some hypothetical cases, focusing on how the various exceptions will influence supervisory authorities, controllers and processors. Finally, I will summarize my findings; that while the mechanism may improve the status quo, it falls somewhat short of fulfilling the promises from EU legislators.

---

[63] Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st Century /* COM/2012/09 Final */ (2012)

[64] Ibid.

[65] Commission Staff Working Paper Executive Summary of the Impact Assessment (2012) Page 5.

#### 4.2.1 The general rule

The essence of the one-stop-shop mechanism is that the supervisory authority where a controller or processor has its main establishment shall be competent to:

- perform various regulatory tasks, exercise various regulatory powers, and take the related decisions concerning that controller or processor, and
- act as a proxy between other supervisory authorities concerned and that controller or processor.

This is primarily regulated in Article 56(1) and (2), and Article 60.

Article 56(1) stipulates that the "[…] supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor […]".

Article 56(6) elaborates on this by establishing that the "[…] lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor".

Article 60 outlines the procedure for cooperation between the LSA and other authorities concerned, and authorizes the LSA to adopt binding decisions.

The crux of these provisions is that a controller or processor only has to relate to one supervisory authority for all of their processing activities in the Union.

This does however raise some questions. First, how to determine what constitutes a "main establishment"? That is to say, what criterion does the Regulation list as relevant for this assessment? And what does "sole interlocutor" mean?

##### 4.2.1.1 *Main establishment*

I will start by looking at the notion of the "main establishment" of an undertaking. The Regulation lists three alternatives for determining what the main establishment is:

First, Article 4(16)(a) defines the main establishment as the place of an undertakings central administration.

Second, if the decisions on the purpose and means of the processing of personal data are taken elsewhere – this establishment is the main establishment.

For both these alternatives, it is worth noting preamble 36, which states that one has to consider whether or not the establishment in question has

effective and real exercise of management activities, if these activities determine the purposes and means of processing, and if these management activities are exercised trough stable arrangements.

This resonates back to recitals 18 and 19 in the preamble to the Directive and the interpretation in Weltimmo, where the Court states that "[…] it should be considered that the concept of 'establishment', within the meaning of Directive 95/46, extends to any real and effective activity — even a minimal one — exercised through stable arrangements."[66]

One cannot necessarily apply the Courts findings in Weltimmo to the Regulation directly. In Weltimmo the broad interpretation of the term "establishment" was in the interest of the data subject – and as such in line with one of the main goals of the Directive. One might imagine situations where a similarly broad interpretation of the "main establishment" criterion in the context of the Regulation might have the opposite effect by allowing an undertaking to establish itself in a desired jurisdiction to the detriment of data subjects at a low cost (so called "forum shopping", which some supervisory authorities has raised concerns about)[67]. Some scholars fear that "[s]uch regime shopping – quite common in matters of tax regulations – might then also occur in terms of data protection. This is already happening, for example, in Ireland, where there are low taxes and low data protection interests united and where big players in the worldwide web already have headquarters as the Financial Times reported on September 25th, 2013 (eBay, Facebook, Google, LinkedIn, Twitter, Yahoo, Accenture, :::)".[68]

On the other hand, a key policy objective is also to ensure "[…] legal certainty and transparency for economic operators […]"[69]. And while these and similar objectives have been given less weight in case law under the Directive, one cannot ignore the importance given to these objectives in the various policy documents and preparatory works to the Regulation.

Finally, the consideration for intra-Union legal consistency and predictability is a substantial argument for interpreting the term "establishment" similarly across various legal instruments and time, continuing the interpretation in inter alia Weltimmo.[70][71]

I find that the key element to take from the Courts case law in this area, is its willingness to apply a teleological interpretation to ensure that the over-

---

[66] Case C-230/14 (Weltimmo) para. 31.
[67] Barnard-Wills, Chulvi and De Hert (2016) page 590.
[68] Fritsch (2015) page 164
[69] The Regulation, Preamble 13.
[70] Case C-230/14 (Weltimmo)
[71] See also WP29 Opinion 8/2010 on applicable law page 11 on "effective and real exercise of activity trough stable arrangements" in the directive, and the relation to the notion of "stable establishment" in case law.

all objectives of the legislation are met. When it comes to the phrase "main establishment" in the Regulation, there will necessarily be a tension between the two conflicting goals of ensuring practical solutions for undertakings, and ensuring that the rights of data subjects are respected. As a preliminary conclusion, I do believe that the flexible interpretation of "establishment" must be continued.

Third, is the question of controllers and processors without a central administration in the Union, and how to determine where the "main processing activities" take place. The preamble does not expand on how to determine this question. There are several reasonable ways of interpreting the phrase, inter alia:

- the processing activities generating (directly or indirectly) the most income for the undertaking in question.
- the processing activities involving the most data subjects.
- the processing activities involving the largest data volumes

The question of what "main processing activities" entails will be a discretionary and overall assessment, likely based on criteria as those listed above. Controllers and Processors would probably be served by a more detailed and elaborate definition of this in the preamble.

#### 4.2.1.2 *Sole interlocutor*

The next question is the definition of "sole interlocutor" in Article 56(2). Oxford Learner's Dictionary defines interlocutor as "[…] a person or an organization that talks to another person or organization on behalf of somebody else".[72]Similarly, the Cambridge Dictionary defines it as someone "[…] who is representing someone else […]".[73]

I interpret this to mean that when one of the national supervisory authorities need to contact a controller or processor, they will have to use the relevant LSA as a proxy for communication with the relevant controller or processor.

The use of the word "sole" seems to imply that controllers and processors will not have to deal with any other supervisory authorities but the competent LSA. That is however not the case, as we will see below when discussing the various exceptions.

#### 4.2.1.3 *Summary*

The key points of general rule on the one-stop-shop mechanism are as follows:

---

[72] http://www.oxfordlearnersdictionaries.com/definition/english/interlocutor?q=interlocutor
[73] http://dictionary.cambridge.org/dictionary/english/interlocutor

- A controller or processor engaging in cross border processing of personal data have to deal with one supervisory authority only – the authority where they have their main establishment. This authority is solely competent to make binding decisions concerning the cross border processing activities of controllers and processors. The supervisory authority should function as a proxy between various supervisory authorities concerned and the controller or processor.
- The main establishment for controllers and processors with a central administration in the Union is said central administration, unless the decisions on why and how personal data is processed is taken elsewhere – then this latter place is the main establishment.
- The main establishment for controllers and processors without a central administration in the Union is the place where the main processing activities take place. This is most likely the place where the processing activities that generates the most income and/or involves the most data subjects take place.

#### 4.2.2 Exceptions to the general rule

We have established that the general rule seems relatively straightforward: Controllers and processors need only to deal with the LSA for their cross border processing. If concerned supervisory authorities need to communicate with such a controller or processor, they will have to go through the LSA, and it is only the competent LSA that make decisions concerning said controller or processor.

There are however several exceptions to this general rule. I have chosen to look closer at the following:

- Processing pursuant to legal obligations, in public interest and by public authorities
- Processing with national impact only
- Urgent cases
- Certain practical/procedural exceptions in connection with initial stages of investigating complaints and similar issues
- Cases involving both controller and processor

I will start by describing and critically assessing these exceptions. Then I will do an overall assessment of the impact of these exceptions – concluding that they do have a non-insignificant impact on the mechanism.

##### 4.2.2.1 *Processing pursuant to legal obligations, in public interest and by public authorities*

Article 55(2) mandates that when processing is necessary for:

- compliance with a legal obligation;
- the performance of a task carried out in the public interest; or
- exercise of official authority,

article 56 on the competence of the lead supervisory authority does not apply.[74]

The fact that the provision concerns the actual processing operation – "[w]here processing is carried out […]" – implies that this exception also applies to processing carried out by processors on behalf of a public authority when the processing is carried out on the basis of point (c) or (e) of Article 6(1).

This exception may have substantial impact for many controllers and processors. Many public authorities – like tax administrations, municipalities or public road administrations, have sizeable processing operations on the basis of both point (c) and point (e) of Article 6(1). These – and similar public administrative bodies – outsource (sometimes substantial) parts of their processing operations to private processors. For instance, Evry conduct several processing operations for the Norwegian Tax Administration. Similarly, Helse Sør-Øst are currently planning to outsource large parts of the operation of their IT systems.

It is clear from the wording of the provision that in these situations, Article 56 – and the one-stop-shop scheme – does not apply. This means that many controllers and processors will have to deal with supervisory authorities other than the competent LSA.

The exception applies for processing based on compliance with a legal obligation to which the controller is subject. A typical legal obligation is that of employers to file employee data for later disclosure to tax or welfare authorities. For controllers having establishments with employees in countries other than that of their main establishment, the one-stop-shop mechanism does not cover processing of this kind. These are processing operations that most, if not all, undertakings established in more than one Member State perform. It is therefore exceedingly likely that this exception will affect many undertakings.

This means that for some companies, part of their processing will be supervised by the competent LSA. Yet for other parts of their operation, the competent supervisory authority will be the national authority in the territory of the public authority concerned. There might even be instances where a processor processes data for the same customer both based on point (c) or (e) of Article 6(1), and based on for instance consent, as part of an ordinary contractual, commercial relationship. Here, a processor would have to relate to two different supervisory authorities for different processing operations, for the same customer.

[74] Article 55(2) refers to processing based on Article 6(1) (c) and (e).

One key advantage with this exception is that the processing is based on legal instruments that the national supervisory authority is closer to understand and apply. The national authority will also often have a better understanding of cultural and social context framing these rules.

#### 4.2.2.2 *National impact – Article 56(2)*

If the subject matter of an infringement only relates to an establishment in a Member State, or substantially only affects data subjects in a Member State, the national supervisory authority concerned shall be competent to handle the case. This starting point is modified by Article 56 para (3) to (5) which authorizes the competent LSA to decide whether it or the national supervisory authority should handle the matter.

In short, these provisions give national supervisory authorities the right to handle purely local matters – regardless of the general rule in Article 56(1) – unless the LSA decides to settle the matter itself.

If the LSA decides to intervene, it must take into account the opinion of the national supervisory authority. If it chooses not to do that, the Board must resolve the dispute.

In the following I will describe the provision in more detail.

The provision states that a national supervisory authority "[…] shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State".

The provision has two alternative conditions:

The first alternative is that the subject matter of a complaint must relate only to an establishment in one Member State – the context implying that this must be a branch or subsidiary of the main establishment in a different Member State in the Union. The wording of this provision is unambiguous and leaves little room for interpretation. Both the word "must" and the word "only" indicate that this is a narrow and clearly delineated exception.

The second alternative concerns subject matter substantially affects data subjects only in one Member State. This provision is somewhat more ambiguous. The wording can mean that the subject matter may affect data subjects in other Member States – as long as it does not do so to a substantial effect. This may create some doubt as to what the provision covers. Consider this hypothetical example: a social media network creates a special 17th of May function that makes it possible to share their pictures/memories. A possible infringement would for the most part affect people in Norway, but

it could also affect some people in other parts of the world. If it substantially affects a few data subjects outside the one country – is that enough? Or must the number of data subjects outside the Member State also be substantial?

The fact that this is an exception to the general rule – and an exception to an important principle in the Regulation – suggests that one should interpret the provision narrowly. In other words: if there is doubt regarding whether or not a processing activity substantially affects data subjects in other Member States, one should revert back to the general rule: the one-stop-shop mechanism.

At the same time, one of the main objectives of the Regulation is the protection of fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data. This suggests that one should interpret the provision more broadly to ensure a better balance of interests. National supervisory authorities will often be closer to the subject matter at hand, and have a better understanding of cultural and social aspects which might impact the case.

I believe that the question boils down to a discretionary and overall assessment closely related to the actual case in question, and that it is hard to say something conclusive at this point. Such an assessment will most likely look at a wide range of different factors including the categories of data processed, the number of data subjects affected, if the controller or processor have profited on the processing operation in question etc.

This exception is subject to an exception in itself. The national supervisory authority must inform the LSA about the possible infringement. The LSA may then decide to defer to the national supervisory authority, or decide to handle the case itself pursuant to the procedure provided in Article 60. I interpret this to be up to the LSA's discretion, but preamble 127 does point at effective enforcement of a decision vis-à-vis the controller or processor as a relevant consideration, creating a partial framework for the assessment.

If the competent LSA decides to handle the case, it must "[…] submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views […]". The national supervisory authority concerned may "[…] [express] a relevant and reasoned objection to the draft decision […]". If the LSA does not take this relevant and reasoned objection into account, the matter is referred to the consistency mechanism referred to in Article 63 resulting in a binding decision from the Board. Furthermore, if the LSA decides to handle the case, the national supervisory authority may submit a draft decision. If the national supervisory authority submits such a draft decision to the LSA, the latter must take utmost account of that draft when preparing the draft decision discussed above. If the LSA decides not to handle the case, the national supervisory authority responsible must

follow the provisions on Mutual assistance and Joint operations of supervisory authorities in Articles 61 and 62.

As I have shown above, Article 56(2) to (5) outlines a rather convoluted process which will – at least until there is more case law, supervisory authority practice and practice from the Board – reduce legal predictability and increase the administrative burden for the controllers and processors concerned.

It is worth noting that preamble 131 appears to suggest an alternative approach in Article 56(2) cases where a:

- possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged; or
- the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States.

In these instances, the supervisory authority concerned should "[…] seek an amicable settlement with the controller […]", and if this does not prove successful, "[…] exercise its full range of powers […]". This seems to outline a procedure bypassing the competent LSA, giving the national supervisory authority the ability to exercise its full range of powers pursuant to Article 57 and 58. It is not immediately clear what the relation between this procedure and the abovementioned procedure involving the LSA is – or what the material differences are. On the basis of the clear and unambiguous wording of Article 56 para (2) to (5), I choose to interpret preamble 131 restrictively, presuming that this mechanism also requires the approval of the competent LSA. The wording of this preamble is nevertheless likely to create confusion.

On the surface, this exception appears like an attempt at fixing a mostly political issue – the Member State's desire to retain a certain amount of national self-determination – in a fairly elaborate legal fashion. It will be interesting to see how the dynamic between lead and concerned supervisory authorities will pan out. Preamble 131 is also a wildcard which reduces legal certainty.

#### 4.2.2.3 *Urgency procedure*

Article 66 permits exceptions to the one-stop-shop mechanism when there is an urgent need to act in order to protect rights and freedoms, and when the ordinary one-stop-shop mechanism might not provide results swiftly enough.

This exception is applicable only in exceptional circumstances. A contextual and linguistic interpretation indicates that the scope of this exemption

clause is very narrow. Also worth noting, is that the exception is limited by a maximum three-month period of validity. Finally, the exception only opens up for measures intended to produce legal effects on the supervisory authority's own territory, which limits the impact for the concerned controllers and processors.

At the same time, the supervisory authority concerned "may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision". Such a binding decision must be handed down within two weeks. A prerequisite for such a request is that the lead competent supervisory authority has not taken appropriate measures in a situation where there is an urgent need to act. The Board must decide whether the competent supervisory authority has taken appropriate measures, and whether there is an urgent need to act. While the provision does not state so explicitly, a contextual interpretation indicates that these urgent binding decisions have permanent effect (compare to Article 66(1) where the period of validity is explicitly limited to three months for the provisional measures).

The very narrow scope of the exception may result in the provision having a very limited practical impact. On the other side, the potential consequences of an urgent binding decision from the Board increases its importance. Furthermore, the Board and other supervisory authorities concerned cannot censor the temporary provisional measures in advance, giving the concerned supervisory authority a certain room for maneuverer.

Overall, I suspect that the various supervisory authorities will use this provision sparingly. At the same time, it allows for national supervisory authorities concerned dealing with controllers and processors directly, and as such, it serves to undermine the one-stop-shop mechanism by reducing the predictability for the concerned controllers and processors. It also increases their administrative burden – having to have procedures in place to deal with more than one supervisory authority. At the same time the exception may increase the level of protection for data subjects. In a digital context, personal data breaches are a question of urgency, and this exception ensures that a national authority might take action faster than what the competent LSA might.

#### 4.2.2.4 *Tasks and responsibilities*

There are two somewhat interlinked issues concerning the various tasks and powers listed in Articles 57 and 58 in the Regulation.

The first issue, is the question of what a national supervisory authority can do in the initial stages of an investigation – before the status of competent LSA is established. Can such an authority monitor the behaviour of a con-

troller if they suspect a violation? Can they impose a temporary, or even a permanent ban on certain processing activities?

The second issue is the more general question about who has what tasks and powers pursuant to Articles 57 and 58. Initially, these Articles seem to indicate that they assign these tasks and powers to the various national supervisory authorities on their territory – which would run counter to the one-stop-shop mechanism. Such an interpretation would leave the LSA with the power to adopt binding decisions pursuant to Article 83 – administrative fines – only.

I will discuss the question of the competence of a national supervisory authority in the initial stages of an investigation first.

One can assume that in many cases, the question of competent LSA will not necessarily be obvious from day one in an investigation. This is somewhat similar to one of the question answered in the Weltimmo-case, where the Court states that when "[…] a supervisory authority receives a complaint, in accordance with Article 28(4) of Directive 95/46, that authority may exercise its investigative powers irrespective of the applicable law and before even knowing which national law is applicable to the processing in question"[75].

I believe a similar principle must apply concerning investigative powers before the identity of the competent LSA is established.

This means that when a supervisory authority receives a complaint, it may exercise its investigative powers pursuant to article 57 and 58, irrespective of whether it is the LSA in the case, until this question is resolved.

There are a wide variety of tasks and powers which might be relevant in such cases, inter alia the following:

- handle complaints and investigate the subject matter, and if necessary coordinate with another supervisory authority;
- ordering the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- imposing a temporary or definitive limitation including a ban on processing.

As a practical example, this problem would come to a head if the Norwegian supervisory authority receive a complaint about Company A, and it is unclear whether A has a central administration in the Union or not – and if so, where it is. It makes sense that the Norwegian supervisory authority should conduct investigations on the application of the Regulation in the

[75] Case C-230/14 (Weltimmo) para. 57

actual case, or notify the controller or the processor of an alleged infringement and take other diligent and necessary steps to avoid further potential violations. At least until they have established where the main establishment of A is.

At the point where the competent LSA has been established, it must resume the position as the sole interlocutor between A and the concerned supervisory authority.

I must underline that this question is not explicitly governed in the Regulation, and that this is part speculation from my side. Policy considerations do, however, dictate that this issue is solved. Furthermore, the Court has, as described above, chosen a similar approach in an analogous case.

To summarize, controllers and processors will most likely have to deal with various national supervisory authorities in initial stages of cases. This will serve to increase the administrative burden of the concerned undertakings.

The second question is which tasks and powers belongs to the LSA, and which tasks and powers belongs to the various national supervisory authorities – after the initial stages of an investigation or case.

As discussed above, the competent LSA is tasked with being sole interlocutor between the establishment in question and the various national supervisory authorities, and the authority competent to make binding decisions. At the same time, Articles 57 and 58 empower the various national authorities by giving them tasks and powers. The question is which – if any – of these tasks and powers are the national supervisory authorities competent to perform and have, in cases where they are not the LSA?

Article 57 explicitly states that "[…] each supervisory authority shall on its territory […]" monitor, promote awareness, advice etc. Article 58(6) states that "[e]ach Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3", clearly indicating that it is the national authority which have these responsibilities, duties and powers on their territory.

At the same time, a teleological and contextual interpretation indicates that it is the LSA that must be competent to make the decisions and carry out the various task. The wording of Article 60(2) supports this interpretation – describing joint investigations or monitoring the implementation of a measure concerning a controller or processor established in another Member State as the responsibility of the LSA. Furthermore, Article 60(7) specifies that it is indeed the lead supervisory who shall adopt binding decisions.

Interpreting these provisions in light of the official policy objectives, and the objectives in the Regulation itself – namely strengthening the convergence

of the economies within the internal market – would also indicate that these tasks and powers belong to the LSA.[76]

Lastly, preamble 130 seems to clearly stipulate that it is indeed the competent LSA that has the authority to both investigate complaints and take measures intended to produce legal effects.

To conclude, the competent LSA has the competence to both perform the tasks outlined in Article 57, and to use the powers outlined in Article 58 (unless exceptions apply – of course).

#### 4.2.2.5 *Cases involving both controller and processor*

For cases involving both a controller and a processor, the competent LSA is that of the Member State where the controller has its main establishment.[77] In such cases, the one-stop-shop mechanism does not apply for the processor if its main establishment is not in the same place as the controller.

This might have large practical consequences for the processors concerned. Some companies specialize in processing data on behalf of controllers. An example is various forms of content delivery network systems or backup services. For these processors, this exception may potentially have a major impact.

At the same time, it is hard to see how this could have been solved differently. An alternative would be to mandate a cooperative procedure between the two supervisory authorities, but that would further undermine the one-stop-shop mechanism, and could prove to further reduce the legal predictability for those involved.

### 4.2.3 Hypothetical processing situations

It can be difficult to look at the exceptions discussed above and understand how they will apply in real life. In this subchapter, I will present a few practical examples illustrating the impact of the exceptions.

#### 4.2.3.1 *Processing pursuant to legal obligations, public interest and by public authorities*

Company A has their main establishment in Germany. In addition to their processing activities in Germany, they provide processing services for various actors in different EU countries. They offer, amongst other things, content delivery network services to both the public and private sector.

---

[76] The Regulation, preamble 12.
[77] Ibid, preamble 36.

In France, they provide hosting services for a public authority, allowing citizens to both send and receive personal data to and from the public authority. The processing is based on Article 6(1)(e) in the Regulation.

The French supervisory authority receives a complaint from a user concerned about a data leak. The French authority is – pursuant to Article 55(2) – competent to handle the matter concerning this particular processing situation. As a result, company A has to deal with the French authority for this processing operation, and the German authority for their overall processing (unless other exceptions apply).

Concurrently, company A has various branches established in other Union countries. These have local employees liable to taxation. Due to the exception in Article 55(2), company A have to deal with the national supervisory authorities in all these countries for the filing of employee data for later disclosure to tax authorities.

This example shows that this exception will affect all controllers and processors with employees in more than one member state, and that it as such does not aid in simplifying the regulatory environment.[78] On the contrary, the exception reduces legal certainty for the concerned controllers and processors and increases the administrative burden for the concerned substantially compared to a one-stop-shop mechanism without this exception.

#### 4.2.3.2 *Processing with national impact only*

In this example, Company B provides tailor made storage and network services for businesses. They have their main establishment in Germany, but have an establishment in Italy, where they have contracted with several of the largest employers in the country to both develop and host a service registering and systematizing employee appraisal interviews.

The company are using Italy as a market test for this service in Europe, and have not marketed or provided this service to any other countries in the Union.

One employee directs a complaint about Company B's security of processing to the Italian supervisory authority, citing a lack of adequate technical and organisational measures for ensuring security of processing. As mentioned above, Article 56(2) gives national supervisory authorities the right to handle purely local matters unless the LSA decides to consider the matter themselves.

---

[78] Granted that one considers that they are established there, but in light of the interpretation of the notion of establishment in Weltimmo discussed above, the likelihood of considering such an arrangement an establishment is high.

The Italian supervisory authority receives the complaint, and starts investigating the case, gathering evidence from – and communicating with – company B. Company B in turn, believe that the German authorities should handle the case.

As a result of the input from company B, the Italian authority contact the German authorities stating that they consider the case to substantially affect data subjects in Italy only, invoking Article 56(2).

The German supervisory authority decides to handle the case themselves, following the cooperation and consistency mechanism in chapter VII of the Regulation which, inter alia, includes paying heed to the reasoned objections to a draft decisions made by supervisory authorities concerned.

The complainant is dissatisfied with this, and contacts the Italian supervisory authority, pointing at out that pursuant to preamble 131, "[…] the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers […]". This statement from the preamble seems to indicate that the Italian supervisory authority is entitled to bypass the approval of the German supervisory authority and proceed with the investigation without further ado. The Italian authority asks the Board to resolve the dispute pursuant to Article 65(1)(a).

This example is meant to highlight two things:

- the national impact mechanism introduces increased uncertainty and reduces the practical foreseeability for the involved parties – even if the legal certainty is adequate; and
- preamble 131 introduces legal uncertainty and might create confusion for both supervisory authorities and commercial actors – at least until the issue is clarified by the Board or the Court.

At the same time, this exception enables the supervisory authority closest to the relevant social, cultural and legal norms relevant for the processing in question, to handle such cases. This is likely to improve the protection of data subjects.

#### 4.2.3.3 *Urgent cases*

Company C deals in pharmaceutical research and the manufacture of pharmaceuticals. They have their main establishment in Ireland, but have subsidiaries in several Member States. A Swedish celebrity discovers that a local newspaper has received very detailed information about their health status. The celebrity partook in a pharmaceutical trial at company C in Sweden some months back, and therefore considers C a natural suspect.

The Swedish supervisory authority considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects. They base their decision partially on the sensitivity of the personal data processed, and on the seeming lack of adequate technical or organisational measures to ensure security of personal data. Furthermore, the authority considers that that there is an urgent need to act, due to the lack of appropriate measures taken by the Irish supervisory authority.

The Swedish supervisory authority chooses to immediately adopt provisional measures towards company C – mandating that they take steps to alleviate the issue regarding processing activities in Sweden. Furthermore, the Swedish supervisory authority requests an urgent binding decision from the Board, citing the risk to the data subjects due to the lack of information security measures.

In this case, company C must deal with

- the Swedish supervisory authority, concerning the provisional measures;
- the Irish supervisory authority, for their day to day processing activities across Europe; and
- the Board, concerning the potential binding decision.

As discussed above, this exception will most likely be sparingly used, at the same time the consequences when it is used are considerable for those involved. This makes the exception, while narrow in scope, important.

At the same time the ability for the national supervisory authority to take action rapidly is vital for data subjects since it may ensure that further infringement is avoided.

#### 4.2.3.4 *Certain practical/procedural exceptions in connection with initial stages of investigating complaints*

Company D offers backup solutions to private customers in Denmark.

A customer suspicions about company D selling personal information to advertisers, and submits a complaint to the Danish supervisory authority.

The Danish supervisory authority initiates an investigation into the affairs of company D pursuant to Article 57(1)(f) in the Regulation, and requests the necessary information pursuant to Article 58(1)(a), due to the outcome of the evaluation of said information, they subsequently impose a temporary limitation on the processing of company D.

Company D raises an objection to the Danish authority, claiming that it is the German supervisory authority that is the competent LSA. The Danish supervisory authority continues its investigation, while concurrently con-

tacting the German supervisory authority to establish which authority is competent to lead the case.

A few weeks into the investigation, the German and Danish authorities amicably decide that it is indeed the German authority, that is competent to be LSA – and they take over the investigation.

This illustrates that even when the one-stop-shop mechanism does apply, it might not apply right away. This exception will probably hit small and medium businesses hardest, as they are more likely to have sporadic and less stable processing activities. The exception also means that supervisory authorities need to coordinate and collaborate efficiently to decide competent LSA as quickly as possible. There is a risk that this exception may also delay the process and as such potentially weaken the protection for the concerned data subjects.

#### 4.2.3.5 *Cases involving both controller and processor*

Company E has their main establishment in Germany. They offer a wide array of various processing services across Europe. In Greece, they have a data processing agreement with company F concerning the processing of various patient files on behalf of company F. Company F has their main establishment in Greece.

A large data leak draws suspicion towards both companies, and the Greek data supervisory authority start an investigation. Pursuant to preamble 36 in the Regulation – which states that the "[…] competent LSA should remain the supervisory authority of the Member State where the controller has its main establishment" in cases involving both a controller and a processor, the Greek supervisory authority is the lead authority for both the controller (company F) and the processor (company E).

This leads to yet another situation where the competent LSA will not be the sole interlocutor for a company. This increases legal uncertainty, and is suitable to create confusion for the concerned processors. At the same time, it ensures a higher degree of predictability for the concerned controllers.

#### 4.2.3.6 *Summary – hypothetical processing situations*

Through these hypothetical examples, I have shown that the one-stop-shop mechanism does not preclude having to deal with supervisory authorities outside of the competent LSA.

Depending e.g. on the type of processing; what the basis of the processing is, what stage in the investigation a case is in; who you process data on behalf of – controllers and processors may have to deal with several supervisory authorities. These exceptions will apply in varying degree to most undertak-

ings with establishments in more than one Member State, and undertakings without an establishment in the Union, but with processing activities in more than one Member State.

It is furthermore worth noting that many of these exceptions are of a nature that makes it hard – or even impossible – for undertakings to ensure compliance (in this context meaning avoiding the exceptions by organizing their operation in a certain way). The key to this situation for all parties involved, is to be aware of the various exceptions, know when they apply, and plan both technical and organisational measures accordingly. Inter alia: if you are an undertaking with establishments in 15 different Member States, and you process your tax related employee data in each country pursuant to various national legal obligations, it would be prudent to be aware of the exception in Article 55(2) (processing necessary for compliance with a legal obligation or processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority), what consequences that exception has for your processing activities and make the necessary technical and organisational adaptations accordingly.

#### 4.2.4 Summary – the relationship between the general rule and the exceptions

As I have established above, the LSA is competent to inter alia:

- adopt binding decisions concerning a controller or processors cross border processing – regardless of where in the Union it takes place;
- be the sole authority communicating with controllers and processors engage in cross border processing, acting as a proxy between these undertakings and concerned supervisory authorities;
- perform a wide range of tasks like monitoring, investigating and enforcing the Regulation; and
- exercise a wide range of powers, like issuing warnings, ordering the controller or processor to provide information;

At the same time, the various exceptions lead to situations where national supervisory authorities have a wide range of tasks and powers in the early stages of a cases, or in special types of case where national supervisory authorities – which are not the LSA – are competent to handle cases directly. This applies to inter alia the national impact rules and the urgency procedure, for processors when the controller is established elsewhere etc.

This creates a tension between one the one hand the general rule of the one stop mechanism, and these exceptions. This tension will serve to undermine the one-stop-shop mechanism by reducing legal certainty and practical foreseeability. For undertakings not established in the Union – and maybe not familiar with EU data protection law – it is not necessarily obvious what a "main establishment" is, and why it does not matter what their main establishment is if they process data on behalf of a public authority for certain

purposes. In light of the new scope of EU data protection law, these companies are in a particularly vulnerable position, not having had to relate to EU law at all previously – now having to deal with its full force.

And while many of these exceptions are justified by policy considerations like efficiency (the urgency procedure) or sovereignty (the exception on public authorities etc.), the sum of the various exceptions results in a far less comprehensive and homogenous mechanism than what the different political objectives discussed above may have alluded to.

The main question after this is whether the Regulation simplifies the regulatory environment by drastically cutting red tape and doing away with formalities, thus eliminating unnecessary costs and reducing administrative burden.

The exceptions discussed above introduce new elements of both red tape and formalities into the Regulation compared to what one may have been lead to believe based on the policy objectives published by the EU legislature. These elements will therefore most likely increase the costs and the administrative burden compared to a hypothetical regulation without these exceptions.

At the same time, it is worth mentioning that these exceptions serve legitimate aims in themselves, increasing the level of protection for data subjects by inter alia ensuring that the authorities most fit to handle certain cases are competent to do so, and by ensuring that processing operations with special circumstances are treated accordingly.

# 5 Discussion, conclusions and observations

In this section, I will summarise my findings in light of my research questions:

- Has the scope of EU data protection law extended in the new Regulation compared to the current Directive?

- Will the one-stop-shop mechanism adopted in the Regulation fulfill the promises of the EU legislature, and reduce administrative burdens, facilitate more efficient cross border flows of personal data and increase legal certainty for controllers, processors and supervisory authorities?

## 5.1 The scope of EU data protection law in the Regulation and the Directive

The first research question in my thesis was the following:

Has the scope of EU data protection law extended in the new Regulation compared to the current Directive?

The short and simple answer to this question is: yes! Undertakings not established, nor using means of processing in the Union area, are not covered by EU data protection law today. When the Regulation takes effect, they most certainly will be – granted that they target data subjects in the Union.

The simplest way to describe the change from the Regulation to the Directive is that the scope of European data protection has increased, and the link between Union territory and the scope of the law has been completely severed.

The Directive links the scope of EU data protection law to the Union territory. It either requires an establishment, or means in one (or more) Member States. The Regulation on the other hand, removes this link between scope and the physical territory of the Union. The Regulation extends the scope of the EU data protection law to processing of personal data by controllers or processors not established in the Union if they target Union data subjects.

This is both a principal and practical departure from status quo – even considering the flexible approach of the Court in both Weltimmo and Google-Spain cases.[79]

Going into somewhat more detail, the chosen approach for extraterritorial scope in the Regulation is to target establishments that choose to target their Union data subjects with their activities. Either by offering their goods or services to data subjects in the Union (Article 3(2)(a)), or by monitoring the behaviour of data subjects in the Union (Article 3(2)(b)).

By example, this means that a online marketplace in the US not actively targeting Union customers, but still get occasional customers from the Union, is not covered by the scope of EU data protection law.[80] Similarly, a social media service tracking European tourists on a road trip in the US, will not be covered by the scope of EU data protection law. Conversely, this also ensures that the scope of EU data protection law cover companies like for instance Target or J. Crew, to the extent that they target the EU market with their services and goods.[81] Likewise, a social network based in for instance South Korea tracking your behaviour from day to day – in the Union – is covered.

Some scholars are critical of this development, and inter alia argue that this new direction "requires substantial refinement to avoid ending in frustra-

[79] Case C-131/12 (Google Spain) and Case C-230/14 (Weltimmo).
[80] See chapter 3.2.3 for a closer examination of when undertakings are considered to offer services or goods to subjects in the Union.
[81] Providing EU currencies, having pop-ups stating "we have made it easier to shop from your country", providing expedited customs handling tailor made for EU countries etc.

tion; the benefits of the 'targeting' test as currently articulated are largely illusory, and the severity of its downsides will no doubt become clear once we see it applied in practice in the data privacy context".[82] While others are more positive to the solution where "you might be targeted by EU law only if you target".[83]

I believe that this solution gives companies a choice – if they want to partake in the economic opportunities that lie within the Union, they must also accept to be covered by the scope of EU data protection law. Similarly, if they want to monetize the personal data of Union citizens, they must accept the added burden of compliance with Union law.

In my view the new approach strikes a reasonable balance between a strict territorial approach, and an approach where all activity involving data subjects in the Union are covered. The former would undermine the protection of Union subjects and almost encourage circumvention. The latter would be a matter of jurisdictional overreach by in practice granting EU data protection law a global scope without prejudice. The chosen approach ensure that the protection of EU data protection law extends to all the data subjects in the Union if they are targeted by establishments outside the Community area, and as such it increases the scope of protection compared to the Directive without unduly extending EU jurisdiction.

### 5.2 Legal certainty, predictability and administrative burden for controllers and processors not established in the Union

As for the question of whether or not the Regulation will improve legal certainty, predictability and as such lessen the administrative burdens for controllers and processors; the answer is rather nuanced. My main conclusion is that the Regulation fails to live up to the promises made by the legislature by introducing too many and varied exceptions to the one-stop-shop mechanism.

Compared to the status quo, the one-stop-shop mechanism is certainly an improvement as some processors and controllers might only have to deal with the LSA for their cross border processing. At the same time, while the one-stop-shop mechanism may reduce the administrative burden compared to status quo, it stops somewhat short of the policy objectives published by the EU legislature before adoption – for various reasons. The biggest issue is not one single exception, but the sum of the various exceptions that serve to undermine the heralded comprehensive approach.

The various exceptions influence both data subjects, supervisory authorities, controllers and processors. I believe that controllers and processors not

[82] Svantesson (2015) page 226
[83] de Hert and Czerniawski (2016) page 9.

previously covered by the scope of EU data protection law will most affected by these exceptions, because they are least likely to be familiar with the various legal, cultural and social norms making up the European regulatory context framing the Regulation and shaping its use. For such controllers and processors, the extended scope – and the one-stop-shop mechanism may lead to a new and substantial administrative burden – directly contrary to the goal of eliminating unnecessary costs and reducing administrative burden.

A related matter is that these exceptions are likely to affect small and medium sized businesses disproportionally. In the context of statements like "[t]he data protection reform will stimulate economic growth by cutting costs and red tape for European business, especially for small and medium enterprises (SMEs). The EU's data protection reform will help SMEs break into new markets" made by the Commission leading up to the new Regulation, this is particularly problematic.[84] Large undertakings will most likely have the resources and means to be prepared for the new Regulation come springtime 2018. For small and medium sized businesses, the situation is different. It is conceivable that this might constitute a barrier to entry to the European market for this segment.

The exceptions may also increase the administrative burden for the concerned supervisory authorities, necessitating increased communication and collaboration efforts to ensure that the Regulation achieves its objectives. At the same time, they might increase the protection for data subjects by inter alia avoiding unnecessary delays in urgent situations.

The fact that some key issues are regulated trough ambiguously worded provisions, further reduces legal certainty, and undermines foreseeability, an important policy goal of the EU legislature. This concern inter alia the initial stages of investigations before the competent supervisory authority has been established – a question that is not explicitly regulated at all. Similarly, the question of national impact processing situations where there are incongruities between the text of the Article in the Regulation, and the preamble

Legal uncertainty is one of the problems the EU legislature set out to reduce, and issues like these undermine this objective. Some scholars even suspect that we "[...] may be seeing more red tape instead of the emergence of a common and secure digital space".[85] It is also worth noting that some European supervisory authorities have expressed concerns about the practical implementation of the one-stop-shop principle.[86]

---

[84] Agreement on Commission's EU data protection reform will boost Digital Single Market (2015)
[85] Burri and Schär (2016) page 20.
[86] Barnard-Wills, Chulvi and De Hert (2016) page 591.

In sum, there are grounds for doubting whether the one-stop-shop mechanism succeeds in drastically cutting red tape and doing away with the formalities plaguing the current system. For some controllers and processors covered by the scope of EU data protection law – particularly those without an establishment in the Union – the mechanism may lead to less legal certainty and in fact increase the administrative burden. Considering that the Council considered the one-stop-shop mechanism to be one of two central pillars of the proposal, these are important concerns.[87]

Looking at the various drafts, comments and proposals, it is obvious that the period between the draft in 2012 and the adopted version in 2015 has been filled with strong disagreement and a tug of war between the Commission and the Parliament. The desire for national hands on the wheel has been in conflict with the objective of a strong one-stop-shop mechanism. The former is evident by the following proposal by the Committee on the Internal Market and Consumer Protection in the Parliament:

> "While processing operations covering more than one country can easily be monitored by the main establishment, and should be the responsibility of a single authority, on the basis of a centralised declaration, national processing activities which are managed on a decentralised basis by branch establishments, and which are difficult for the main establishment to supervise, should be the responsibility of each national supervisory authority".[88]

The conflict between protecting the data subjects and protecting business interests is also evident, for instance in the one-stop-shop mechanism proposed by the Committee on Industry, Research and Energy in the Parliament:

> "Where the processing of personal data is the subject of a complaint lodged by a data subject, the competent authority, providing the one-stop shop, should be the supervisory authority of the Member State in which the data subject has its main residence. Where data subjects lodge similar complaints against such processing with supervisory authorities in different Member States, the competent authority should be the first seized".[89]

---

[87] Data Protection: Council Supports "One-Stop-Shop"Principle.
[88] Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (2013) page 27.
[89] Opinion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of

The bottom line is that while one-stop-shop mechanism will prove to be hugely useful for many undertakings, and will presumably reduce administrative burden and fragmentation for many – if not most – undertakings. The mechanism therefore fails to fully live up to the political promises heralding it – primarily because the EU legislators have created a compromise which is neither fully here nor there.

personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (2013) page 36.

# 6 Table of reference

## 6.1 Articles

de Hert, Paul and Czerniawski, Michal (2016) Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context- 2016/07/13 International Data Privacy Law - 10.1093/idpl/ipw008 – http://idpl.oxfordjournals.org/content/early/2016/07/13/idpl.ipw008.short.

Lenaerts, Gutiérrez-Fons (2013) AEL 2013/9 Academy of European Law Distinguished Lectures of the Academy To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice http://cadmus.eui.eu/handle/1814/28339.

Bygrave, Lee A. (2000) Determining Applicable Law pursuant to European Data Protection Legislation http://folk.uio.no/lee/oldpage/articles/Applicable_law.pdf.

Fristch, Clara (2015) Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite. http://link.springer.com/book/10.1007/978-94-017-9385-8

Svantesson, Dan Jerker B (2016) Article 4(1)(a) 'establishment of the controller' in EU data privacy law—time to rein in this expanding concept? – https://academic.oup.com/idpl/article-abstract/6/3/210/2447255/Article-4-1-a-establishment-of-the-controller-in?redirectedFrom=fulltext.

Svantesson, Dan Jerker B (2015) Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the Regulation – https://academic.oup.com/idpl/article-abstract/5/4/226/2404462/Extraterritoriality-and-targeting-in-EU-data.

Kuner, Christopher (2015) Extraterritoriality and regulation of international data transfers in EU data protection law http://idpl.oxfordjournals.org/content/5/4/235.short.

Spiekermann, Sarah, Acquisti, Alessandro, Böhme, Rainer, Hui, Kai-Lung (2015) The challenges of personal data markets and privacy http://link.springer.com/article/10.1007/s12525-015-0191-0.

Burri, Mira and Schär, Rahel (2016) The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-driven Economy https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792222.

Barnard-Wills, David, Pauner Chulvi, Christina, De Hert, Paul (2016) Data protection authority perspectives on the impact of data protection reform on cooperation in the EU.
http://www.sciencedirect.com/science/article/pii/S026736491630084X.

Skouma, Georgia, Léonard, Laura (2015) On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection.
http://link.springer.com/book/10.1007/978-94-017-9385-8

## 6.2 **Laws and regulations**

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Treaty on European Union (Consolidated version 2016) - OJ C 202 (2016)

Treaty on the Functioning of the European Union (Consolidated version 2016) - OJ C 202 (2016)

Charter of Fundamental Rights of the European Union (2016) - OJ C 202 (2016)

Treaty of Lisbon (2007) - OJ C 306 (2007

## 6.3 **Case law**

Case C-131/12 (Google Spain SL and Google Inc. versus Agencia Española de Protección de Datos (AEPD) and Mario Costeja González)

Case C-230/14 (Weltimmo s. r. o. versus Nemzeti Adatvédelmi és Információszabadság Hatóság)

Case 283/81 (CILFIT – in liquidation – and 54 others versus Ministry of Health, in the person of the Minister and Lanificio Di Gavardo SPA.

HR-2010-1734-A - Rt-2010-1197 - A versus Centrebet PTY Ltd.

Joined cases C-585/08 and C-144/09 (Peter Pammer (C-585/08), Hotel Alpenhof GesmbH (C-144/09) versus Reederei Karl Schlüter GmbH & Co KG (C-585/08), Oliver Heller (C-144/09)).

## 6.4 **Decisions**

Opinion 8/2010 on applicable law Adopted on 16 December 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

## 6.5 **Preparatory works**

Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD) C7-0025/12 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Text with EEA relevance) {SEC(2012) 72 final} {SEC(2012) 73 final} http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

Opinion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (2012) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-496.562+02+DOC+PDF+V0//EN&language=EN

Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, 2012 http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009)

Commission Staff Working Paper Executive Summary of the Impact Assessment (2012) http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_73_en.pdf

Commission Staff Working Paper Impact Assessment (2012) http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

2012/0011 (COD) Proposal for a Regulation of the European Parliament And of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Text with EEA relevance) {SEC(2012) 72 final} {SEC(2012) 73 final} - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (2013) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-496.497+02+DOC+PDF+V0//EN&language=EN

Opinion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (2013) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-496.562+02+DOC+PDF+V0//EN&language=EN.

### 6.6 **Various online sources**

Reform of EU data protection rules (2016) http://ec.europa.eu/justice/data-protection/reform/index_en.htm - accessed 27. July 2016

The EU General Data Protection (2016) http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

Data protection: Council supports “one-stop-shop”principle (2013) Council of the European Union, press release, 14525/13 (OR. en) PRESSE 403, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/138924.pdf - accessed 21.10.16.

http://www.oxfordlearnersdictionaries.com/definition/english/interlocutor?q=interlocutor.
http://dictionary.cambridge.org/dictionary/english/interlocutor.

Comparison of the Parliament and Council text on the General Data Protection Regulation https://edri.org/files/EP_Council_Comparison.pdf - accessed 06102016.

Agreement on Commission's EU data protection reform will boost Digital Single Market (2015) http://europa.eu/rapid/press-release_IP-15-6321_en.htm - accessed 5. November 2016.