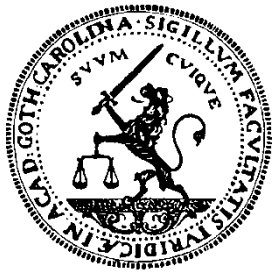

FACULTY OF LAW
Lund University

Rasmus Hansen Jagrelius

The Specific Situation and Needs of SMEs and the GDPR – Taking the account of small enterprises and smaller data subjects

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws program
30 higher education credits

Supervisor: Xavier Groussot

Semester of graduation: VT2019

Contents

Abstract

EN

The General Data Protection Regulation, GDPR, aims to provide protection of personal data which is centred on the data-subject, while at the same time categorically giving special consideration to the specific needs of micro, small and medium-sized enterprises, SMEs. The thesis approaches this conundrum from a fundamental rights angle, and tries to answer how the rights and interests of smaller businesses can be balanced against the rights and interests of data subjects. The thesis examines the GDPR articles and recitals relevant to the SME question, and the self-regulatory systems of codes of conduct and certification; after identifying a number of possible obstacles to the proper balance between rights, the thesis turns to the case law of the CJEU for possible guidance. The thesis finally constructs a three-question test out of case law concerning the relevant rights, and uses this test to discuss possible solutions for overcoming the identified obstacles.

SV

Dataskyddsförordningen, GDPR, ämnar att skydda personuppgifter genom att sätta den registrerades intressen är i fokus, samtidigt som lagen specifikt beaktar mikroföretag samt små och medelstora företags, SMEs, särskilda behov. Uppsatsen närmar sig denna problematik från ett perspektiv baserat på grundläggande rättigheter; problemformuleringen är hur mindre företags rättigheter och intressen kan balanseras mot datasubjektens rättigheter och intressen. I uppsatsen behandlas GDPR-artiklarna och övervägandena som är relevanta för SME frågan, och självreglerande system som uppförandekoder och certifiering. Efter att ha identifierat ett antal möjliga hinder för balans mellan rättigheterna, vänder sig uppsatsen till EG-domstolens rättspraxis för eventuell vägledning. Uppsatsen konstruerar slutligen ett test utifrån rättspraxis om relevanta rättigheter och använder detta test för att diskutera möjliga lösningar för att övervinna de identifierade hindren.

DE

Die Allgemeine Datenschutzverordnung (DSGVO) zielt darauf, den Schutz personenbezogener Daten des betroffenen Personen zu gewährleisten, wobei gleichzeitig den besonderen Bedürfnissen von Kleinstunternehmen, sowie der kleinen und mittleren Unternehmen (KMU), besondere Aufmerksamkeit geschenkt wird. Die Abhandlung geht dieses Problem aus einer Grundrechtsperspektive an, und versucht zu beantworten, wie die Rechte und Interessen kleinerer Unternehmen gegen die Rechte und Interessen der betroffenen Personen abgewogen werden können. In der Abhandlung werden die Artikel und Erwägungen der DSGVO für die KMU-Frage, und die Selbstregulierungssysteme wie Verhaltenskodizes und Zertifizierungen untersucht. Nachdem eine Reihe möglicher Hindernisse für ein angemessenes Gleichgewicht zwischen den Rechten identifiziert worden ist, wendet sich die Abhandlung an die Rechtsprechung des EuGH, um Hinweise zu erhalten. Das Papier baut schließlich einen Drei-Fragen-Test aus der Rechtsprechung zu den relevanten Rechten auf und verwendet diesen Test, um mögliche Lösungen zur Überwindung der ermittelten Hindernisse zu diskutieren.

Preface

The author of this thesis would like to thank Xavier Groussot for his mentoring, Junyi Ren and Lucas Fulanete Gonçalves Bento for their help in the final phases of writing and re-writing, and his mother for her endless patience.

Abbreviations

EDPB	European Data Protection Board
CJEU	Court of Justice of the European Union
DPA	Data protection authority
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
SME	Micro, small and medium-sized enterprise
WP29	Article 29 Working Party

1. Introduction

1.1 Background

In early 2018, the General Data Protection Regulation 2016/679, more commonly known as the GDPR, had something few laws have: the public's awareness. Perhaps that was due to every natural individual having their electronic inbox bombarded by firms asking for the user's consent to keep sending marketing email;[1] perhaps it was due to the Cambridge Analytica scandal, where information had been extracted concerning at least 87 million Facebook users, still being fresh in the minds of consumers and journalists.[2]

This was a stroke of luck for the GDPR that, as the successor to the Data Protection Directive from 1998, would have to take over from a legislation that ultimately fell short of expectations.[3] While the GDPR's content is not dissimilar to the directive's, the newer legislation differentiated itself with a number of key principles. One such principle was making the subject of the data, the data subject, the point of focus for determining the proper level of data protection – the data processing firm's capabilities would theoretically not enter into the calculation.[4] This data subject focus brings us to – one of – the conundrums of the GDPR: while the firm's nature should theoretically not enter into the calculation of the proper level of data protection, the recitals to the law make it clear that, categorically, SMEs' "specific needs" deserve to be considered when it comes to the application of the legislation.[5]

It is clear that SMEs could benefit from some attention. In a survey conducted by the Federation of Small Businesses in February of 2018, less than 10% of small businesses stated that they had finished their preparations for the GDPR; one third stated that they had not even started.[6] In a study published in April of 2018, conducted by the Ponemon Institute, the percent of smaller companies that stated that they expected to be in compliance with the GDPR was significantly below the average of all companies.[7] A survey conducted by TrustArc in July of 2018 concluded that only one in five firms saw their company as GDPR compliant.[8]

---

[1] See "Who will be the main loser from Europe's new data-privacy law?", The Economist.

[2] See "As GDPR nears, Google searches for privacy are at a 12-year high", The Economist.

[3] See "Review of the European Data Protection Directive", RAND Europe, page 7.

[4] See e,g the layout of article 7 and the lack of any reference to the enterprise itself in article 24 of the GPDR.

[5] See recital 13 of the GPDR. The GDPR uses the term "micro, small and medium-sized enterprises", with reference to "Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises". This paper will use the abbreviated term SME.

[6] See "Many small firms are still unprepared for GDPR", Jackson, Olly, page 1-2.

[7] See "The Race to GDPR: A Study of Companies in the United States & Europe", page 2.

[8] See "GDPR Compliance Status A Comparison of US, UK and EU Companies", page 7.

As the authorities move forward, it is likely that the limited resources of the DPAs will be spent on larger actors instead of the vast number of SMEs.[9] The confusion regarding adherence, combined with a predicted lack of enforcement, risks developing into a scenario where many SMEs do not adhere to the GDPR. This has repercussions not only for the data subjects that interact directly with these firms, but also for the economic market of the Union and the structural integrity of the privacy protection the GDPR sets out to create.

Firms are connected, especially when it comes to data security. Cooperating firms often partly link their databases; this creates substantial cost-savings in the day to day operations of the firms, as supply chains, order information and general exchange of data are sped up. However, this also means that one firm's strong data protection can potentially be bypassed by a nonlegitimate actor that has gained access to the database of a firm cooperating with the strongly defended one.[10] A particularly noteworthy case of this is the breach experienced by the American retailer Target in December of 2013, where hackers gained access to personal data of up to 110 million customers after accessing Target's gateway server through a third-party vendor.[11] Simply put, firms cannot effectively cooperate with firms lacking in data security without putting their own data security at risk.

In the possible scenario where many SMEs do not adhere to the GDPR, there will be substantial transaction costs for any cooperation between a smaller and a larger actor, as data cannot be freely transferred between the firms. On top of decreasing efficiency, these increased costs could substantially slow down the market progress towards the unified market of the EU, as larger actors face obstacles in cooperating with smaller local firms to gain a foothold in a new market. The smaller actors in turn lose out on business and long-term opportunities for growth.

When it comes to data security itself, breaches in one actor can lead directly to breaches in another actor, regardless of any cooperation between them. The only requirement is that they share users.

Anonymisation, where various personal identifiers, such as names and addresses, are deleted from the saved data, as well as the weaker pseudonymisation, where the information is separated and kept in another location, are techniques explicitly mentioned by the otherwise technologically neutral GDPR, as appropriate measures in protecting personal data.[12] However, through what is commonly referred to as "de-anonymisation", nonlegitimate actors can access personal data from datasets that have been scrubbed from identifying

[9] The Swedish DPA, Datainspektionen, has, as of 2019, about 80 employees according to their website's "About us" section. Compare this to the roughly 686 000 SMEs in Sweden, according to Eurostat.

[10] See "Symantec Corporation Internet Security Threat Report 2013", page 4.

[11] See "Anatomy of the Target data breach: Missed opportunities and lessons learned", Michael Kassner, ZDNet, Feb 2 2015.

[12] See recital 28 of the GDPR.

information, removing the protection, and making individuals directly identifiable. There are various techniques, but the basic idea is to find patterns matching already obtained data within the larger dataset that is being attacked. For example, detailed health records could be de-anonymised by matching up treatment dates with records of sick leave obtained from a smaller, under-protected, employee database.

César A. Hidalgo, associate professor at MIT, says that:

> *The space of potential combinations is really large. When a person is, in some sense, being expressed in a space in which the total number of combinations is huge, the probability that two people would have the same exact trajectory [...] is almost nil.*[13]

In a paper from 2009, Narayanan and Shmatikov stated that in their experiments, detailed information of between 30 and 150 individuals were sufficient for de-anonymising networks with 100 000 to 1 000 000 members.[14]

What this means in practice, is that the protection of a certain individual's personal data is, to a certain degree, only as strong as the protection offered by the weakest actor that processes that individual's data.[15] While the non-legitimate actors still need to obtain the data they want to de-anonymise, the problem is that there is in practice no way to remove the data that has been spread and continues to be spread through channels used by nonlegitimate actors. What this means, is that for each data breach that results in the spread of non-altered personal data, this theoretical database available to non-legitimate actors for cross-checking grows, which means that data-altering will gradually become a less and less effective measure. Since the GDPR advocates for anonymisation and pseudo-anonymisation of data as an appropriate way to increase data security, it is in everyone's best interest that the measure remains strong. To effectively slow this development, it will be vital to improve the data protection offered by the weakest actors – which will often be SMEs.

In general terms, data security is every firm's business, regardless of them cooperating directly or just sharing customers. Good actors therefore naturally pressure bad actors to change their behaviour. According to Eurostat, in the EU around 99,8 % of enterprises fell under the SME definition in 2018.[16] By ignoring these firms, a significant opportunity for the market to regulate itself is lost.

However, all this is not to say that there are no specific gains for the SMEs themselves. If there in practice are substantial differences in how firms are treated by DPA depending on the size of the firm, growth may be hindered. Enterprises

---

[13] See "How hard is it to 'de-anonymize' cellphone data?", Larry Hardesty, MIT News Office.
[14] See "De-anonymizing Social Networks", Narayanan, A. and Shmatikov, V., page 6.
[15] This was problem was observed by Sergio Fumagalli at the GDPR conference at Politecnico University, Milan.
[16] See "Eurostat - Statistics on small and medium-sized enterprises".

could intentionally hold off on hiring or expanding their business to avoid regulatory attention, or be forced to break their momentum in expansion by focusing on internal measures, which has proven negative effect on their future growth.[17] In other words, SMEs may face hindrances both to their ability to structure their business, and to their corporate growth.

SMEs have been described as the "financial backbone" of the EU.[18] Various national policies of the member states make it clear that this is also recognised on the national level. Furthermore, in the current climate of a divided union, it is important to note that a larger percentage of workers are employed by a SME in Italy and Poland than the EU average;[19] unequal treatment of enterprises risks exacerbating political friction.

There should therefore be no doubt that the GDPR's effect on SMEs will have repercussions not only on the question of protection of personal data, but also for the economic and political functioning of the EU. Despite this importance, many lawyers working closely with smaller firms feel that the question has been underdiscussed, and that attention has primarily been given to the law's effect on larger firms.

1.2 Purpose and research question

Let us examine what the legislation itself says. The following is a direct quote from recital 13 of the GDPR:

> *To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation*

The GDPR emphasises not only the "specific needs" of SME, but also the "specific situation". The recital serves as a strong indicator that the special care SMEs are to be given is not purely educational. The derogation regarding record-keeping is a concrete rule that eases a real administrative burden. Encouraging Union institutions, bodies, member states, and national DPA to take account of SMEs in specifically the "application" of the GDPR also leaves little doubt that the legislator is aiming for more practical consideration.

What are the "specific situation" and "specific needs" of SMEs? Some proposed characteristics of SMEs are a lack of systematic human resource and business strategies, with the focus instead being on their day-to-day business. SME

[17] See "Growth in Established SMEs" Anders Uddenberg, page 92-95.
[18] See "Eurostat - Structural Business Statistics - Small and medium-sized enterprises (SMEs)".
[19] See "Eurostat - Statistics on small and medium-sized enterprises".

company owners have classified management tools as "too abstract or too bureaucratic".[20]

In the context of the GDPR, if the "specific situation" of SMEs is partly characterised by a lack of overarching management tools, it would be both costlier and more time-consuming for SMEs to gain the oversight and governance so often touted as instrumental in achieving GDPR compliance. This is combined with the tendency of SMEs to focus on their day-to-day business – if few SMEs have a HR department, how many would have one for law? Relying on outside expertise is bound to be costly, comparatively inefficient, and may mesh badly with the GDPR's requirements concerning continuous reviews and updates of security measures.[21] In other words, SMEs lack both the tools and the knowledge to effectively transform the GDPR's numerous key principles into concrete corporate changes. This is not simplified by the GDPR's commitment to being technologically neutral.[22] While this policy, that the law does not categorically favour, nor dis-favour, any particular way to meet its requirements, solves the allegedly common problem of IT law to quickly be made obsolete by technical developments, it also means that SMEs lose out on the practical guidance that formal requirements would have provided.

The CJEU has stated that obligations that restrict the free use of resources at a firm's disposal, or more specifically "obliges [the firm] to take measures which may represent a significant cost for [the firm] and have a considerable impact on the organisation of [the firm's] activities"[23], may encroach upon the freedom to conduct a business, as per article 16 of the Charter. This is especially pressing for SMEs: as was detailed in the paragraph above, the specific situation of SMEs makes it so that the GDPR obligations are both costlier and have a larger impact on a SME's activities than larger firms; consequently, SMEs' freedom to conduct a business is threatened to a higher degree by the GDPR.

However, the purpose of the obligations stemming from the GDPR are clear: to protect the data concerning EU citizens. The fundamental rights aspect here is obvious: citizens of the EU, have a right to respect for respect of private and family life, as per article 7 of the Charter, and a right to protection of personal data, as per article 8. In other words, there is a clash of rights.

What this means, is that while the legislator may have identified the, relative to other firms, larger risk the GDPR poses to SMEs, and therefore the need for special measures to avoid infringing upon these smaller firms' right to conduct a business, these special measures must be shaped while giving respect to the fundamental rights of data subjects.

Thus, before the Union institutions and bodies, member states and their supervisory authorities can incorporate the specific situation and needs of SME into

[20] See "Guide for Training in SMEs", page 27.
[21] See e.g. article 24(1) of the GDPR.
[22] See recital 15 of the GDPR.
[23] Judgment of 30 June 2016, *Lidl*, C-134/15, ECLI:EU:C:2016:498, paragraph 29.

their use of the GDPR, they need to be able to ascertain how these measures – meant to alleviate the infringement upon a SME's freedom to conduct a business – would affect the rights of data subjects interacting with that firm.

While there may be multiple ways to find this balance between the involved rights and interests, this thesis will suggest applying the case law of the CJEU in the way of a formalised test. To illustrate how this could be done, the thesis presents the following three-question test, which in the context of a single firm's data protection measures, can be used to determine the proper balance between business and privacy interests, and with that the appropriateness of the data protection measures.

i. Is the origin of data processing found in the common will of the parties?
ii. Is the data processing compliant with purpose minimisation, data minimisation and storage limitation?
iii. While taking the principle of diminishing returns in account, as well as the answers to the two questions above: are the current data protection measures in the upper limit of what can be done without undue cost and impact on the enterprise's organisation?

This test is constructed out of ideas and lines of thought used by the Court of Justice of the European Union in their judgments involving the fundamental rights of the freedom to conduct a business and the right to respect for privacy and family life and protection of personal data; the specific case law and citations will be presented later in the thesis.

A test of the type proposed would provide two major benefits: [1] greater legal certainty to firms, and [2] safeguarding due consideration to both the freedom to conduct a business and the privacy interests.

Smaller firms, as well as for organisations that advice smaller firms, being able to judge the appropriateness of a specific data protection measure would greatly help in meeting the specific needs of SME, as this would dampen the necessity of overarching management tools and costly, tailor-made solutions for the individual firm, thus alleviating the costs and impact on the individual firm – thereby protecting the freedom to conduct a business, as per the CJEU's reasoning. Moreover, the nature of the test could lead to these benefits being "free" – that is, they would happen without data subjects losing qualitative protection of their personal data.

This thesis will show that this type of tool, exemplified by the three-question test, will be instrumental in meeting the specific SME needs and solving the problems associated with the specific SME situation, while also keeping the proper balance towards the data subjects' interests and rights in mind.

This thesis will do this by first examining the articles and instruments of the GDPR that either directly or indirectly apply to specifically SMEs. Afterwards, having noted the weaknesses of the articles and instruments, the thesis will go to the Luxembourg court's case law for ways to remove or diminish these problems.

In cases where the current case law offers no clear solutions – which are expected to be numerous, with the field being so relatively young – the thesis will examine relevant case law in adjacent fields for what could be the developed into a solution, finally compressing the complete findings into the three-question test, presented above. The thesis will then detail how this three-question test, or something providing similar answers, would be used to remove or diminish the problems noted earlier in the thesis. It is important to note that the three-question test is presented both as a possible course for the CJEU to take, or rather continue on, when it comes to the field of data protection, and as a foundation for future discussion.

This thesis' overall objective is therefore to answer how Union institutions and bodies, member states and their supervisory authorities can properly balance the freedom to conduct a business with the respect for private and family life and protection of personal data when incorporating the specific situation and needs of SMEs into their interpretation of the GDPR and its enforcement.

1.3 Method and sources

In trying to answer this question, the primary source of GDPR guidance is the guideline documents written by the article 29 working group, also known as the WP29. After the GDPR went into force, the WP29 became the European data protection board, the EDPB. At the time of writing, the EDPB has released comparatively little material – the work published by the WP29 is however still valid.[24] When discussing released guidelines and documents, either the WP29 or the EDPB will be referred to as the author for the sake of correctness; the nature of the released material does however not change substantially between the two authorities.

Due to the thesis' focus on enforcement of new regulation, literature directly applicable to the posed question is not yet available. The primary material will therefore be the discussed law itself, as well as material published by various EU organs or affiliates. The supplementary material will be academic papers and reports made by non-EU organisations. Various online sources, such as non-academic articles, blog posts etc., will be used for discussing the newest development and as supplementary material.

The primary methodology will be traditional black letter interpretation. However, a certain amount of interpretation pertaining to corporate viability will be used due to the nature of the posed question and the subject matter.

1.4 Structure

This thesis consists of five sections. The introduction introduces the problem of SME treatment in the GDPR, the gravity and importance of the problem and how the thesis will approach it.

[24] See "The European Data Protection Board Endorsement 1/2018".

The second section will examine the recitals and articles of the GDPR that concern SMEs. The focus will be on the concrete derogation from the record-keeping obligation in article 30(5), and how the article is interpreted by the EDPB and WP29. This interpretation will be critically analysed, and an alternate interpretation will be presented. These two interpretations will then be analysed side by side in their effect on the rest of the GDPR, in the interest of promoting a cohesive and predictable regulation. The section will then move on to the two articles concerning codes of conduct and certification, article 40 and 42 respectively; the articles state that Union institutions and bodies, member states and their supervisory authorities are to take account of the specific SME needs when contributing to the development of both of these tools. The thesis will look at the articles' illustration of the two tools' general functioning in a GDPR context.

The third section will supplement the above by examining codes of conduct and certification outside of strictly a GDPR context: codes of conduct as they worked under the Data Protection Directive, and certification as it currently works in the more general field of data protection. The systems in their the current forms will then be examined in the light of the systems viability in helping the average SME with GDPR compliance. Finally, binding corporate rules, BCRs, will be examined as a part of a critical analysis of how self-regulatory systems interact with the balance of fundamental rights and interests of data subjects.

The fourth section will be spent analysing the case law of primarily the CJEU, to answers questions raised after examining the articles and recitals which concern SMEs. To alleviate the observed problems, the aim is to create a test which can be used to [1] provide greater legal certainty to firms, and [2] do this in such a way that gives due consideration to both the freedom to conduct a business and the privacy interests. Relevant case law will be examined, analysed, and finally condensed into the three-question test presented above.

The fifth section will use the three-question test presented in section four to address the problems observed in prior sections, as well as discussing how the tools chosen for meeting the specific SME needs and helping with the specific situation of SMEs can be used in creating a logical and cohesive system for properly balancing the freedom to conduct a business with the respect for private and family life and protection of personal data. The section will then end with a summary and conclusion of the thesis as a whole.

1.5 Delimitations

While this thesis chooses to examine the articles of the GDPR that pertain specifically to SMEs, and only analyse other areas to provide answers to questions raised by said articles, this is not the only way to approach the problem of SMEs' place in the GDPR. The phrasing of recital 13 technically opens up for the possibility of giving due attention to the specific needs in all areas where there needs to be a unified assessment of the level of data protection needed, such as article 24, 25 and 32. The reason the thesis avoids this approach is partly to avoid losing focus, and partly due to a lack of material to support this more practical approach. While this thesis discusses the appropriateness and merits of individual

personal data protection measures, it only does so on a general and theoretic basis – not on a practical level. This is again to avoid losing focus, but also in the interest of providing a general foundation for future discussion.

2. Relevant recitals and articles for the SME question

2.1 The derogation from record-keeping

In the GDPR, the recitals that directly mention SME are 13, 98, 132 and 167. Out of these, the most interesting one is recital 13, which concerns many of the general aims of the regulation. The three latter recitals concern codes of conduct, awareness-raising activities and commission actions respectively. While a possible interpretation of this is that it is these three areas that are the most important for meeting the specific SME needs, such a deduction quickly runs into a major problem: recital 100, which concerns certification, does not mention SME – while the main certification article in the legislation, article 42, clearly mentions them.

There are two articles in the legislation that directly mention SMEs: articles 40 and 42, relating to codes of conduct and certification respectively. There is not much in the way of practical guidance – the wording of the articles is quite close to the wording in the recitals, stating that the specific needs of SME should be "taken into account".

However, there is an article that indirectly mentions SME – by instead mentioning the most important aspect of its criteria: the organization should employ less than 250 persons. That article is article 30(5).

Recital 13 of the GDPR was earlier quoted regarding a special derogation for SMEs. The legal implementation of that recital is found in article 30(5), which states that: an enterprise with fewer than 250 employees does not need to fulfil the record-keeping obligation of article 30, unless:

i. the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects,

ii. the processing is not occasional, or

iii. the processing includes special categories of data, as defined in article 9, or data related to criminal convictions and offences as defined in article 10; this third point shall hereafter be referred to processing concerning sensitive data.

The WP29 brief guidance on this derogation, running no more than two pages, places the weight on the second point of 30(5): "occasional".

2.1.1 WP29 on the derogation and meaning of "occasional"

On the 19:th of April 2018, the WP29 released a position paper, containing "some clarifications on the interpretation" of 30(5).[25] According to the paper itself, the

[25] "Working Party 29 Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR".

group felt this was necessary after receiving a high number of requests from companies.

The document is not a full working paper and runs no more than two pages. Out of this, the actual guidance is less than a page, which can be accurately solidified into two points. Firstly, 30(5) is not all or nothing – the derogation applies to each processing activity carried out by an enterprise separately. Secondly, the group defines occasional processing as processing that "is not carried out regularly, and occurs outside the regular course of business or activity of the controller or processor".

For further guidance on the meaning of occasional, the WP29 refers to its previously published working paper on Article 49 of the GDPR;[26] which concerns derogations that allow for the transfer of data despite article 45(3) or 46 not being fulfilled.

In their guidelines, the WP29 states that the following situation is an example of "occasional transferring": "if personal data of a sales manager, who in the context of his/her employment contract travels to different clients in third countries, are to be sent to those clients in order to arrange the meetings.".

The WP29 goes on to state that data transfers that are regularly occurring within a stable relationship could be deemed as systematic and repeated, hence exceeding an "occasional" character. The group notes that this precludes many transfers within a business relationship from being occasional.

These guidelines make for a somewhat confusing package: the WP29's single example of occasional processing seems to be incompatible with the guidance given less than a paragraph later, as the example appears to happen within a business relationship, as well as being within the regular duties of a sales manager.

Perhaps the WP29's aim was to make the derogation in 30(5) very limited. Returning to the position paper on 30(5), after giving their clarifications on the interpretation, the group states that record-keeping is "a very useful means" for fulfilling the GDPR duties. It then goes on to recommend the national supervisory authorities to provide tools for easing the burden of setting up and managing the record-keeping. A specific example of this would, according to the WP29, be providing a "simplified model that can be used by SMEs to keep records of processing activities not covered by the derogation". The group does not expand on whether this simplification is in regard to the registration duties in 30(1), or in comparison to some unspecified, more elaborate, record-keeping model – this is perhaps a moot point, as at the time of writing, the EDPB have made no announcements of any such material being released by any national DPA.

[26] "Guidelines on Article 49 of Regulation 2016/679".

The author of this thesis believes that the above reasoning, on both the WP29's interpretation of 30(5) in general and the interpretation of "occasional" specifically, can be criticised on a number of points.

2.1.2 Criticism of the WP29 interpretation

The exact legal meaning of "occasional" is hard to pinpoint – the term is relative to the context it is used in. With the term being used in legislation concerning matters ranging from money-laundering to the international market of bus and coach services, it is clear that cross-field interpretation must be supported by additional arguments. [27] While there may be common factors in the term's use across fields, the term does not have a single, precise definition in EU-law.

In their working paper 262[28], the WP29 stated that "occasional" and "not repetitive" have the same meaning. The terms were discussed together and described as follows:

> *These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. For example, a data transfer that occurs regularly within a stable relationship between the data exporter and a certain data importer can basically be deemed as systematic and repeated and can therefore not be considered occasional or not-repetitive.*[29]

This is a definition that has aspects both concerning character and frequency. Character as far as in concerning "random, unknown circumstances" and frequency as in concerning "not-repetitive". The WP29 implies, in their wording, that they are aware of this by describing a problematic processing as both "systematic" and "repeated". The WP29 starts with describing when the term applies: in situations where the transfer happens more than once but "not regularly" and "outside of the regular course of actions". In other words, for something to be "occasional" it can be described as neither "systematic" nor "repeated". It is not both of these qualities exhibited together that renders the classification of processing as "occasional" impossible – processing having either of these qualities makes the processing or transfer non-occasional. There can therefore be considered to exist a certain point of frequency of processing, which if surpassed, leads

[27] See "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing" and "Regulation (EU) No 181/2011 of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport".

[28] The later "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679", released by the EDPB, copies several paragraphs verbatim from working paper 262, including the paragraph on "occasional" and "not repetitive".

[29] See "Guidelines on Article 49 of Regulation 2016/679", page 4.

the processing to be able to be considered “repeated”, and therefore non-occasional.

Let us return to 30(5), taking things from the top: in the text of 30(5), there are three criteria for the derogation to apply: the processing should not be likely to pose a risk, the processing should not be occasional, and the processing should not concern sensitive data.

Out of these, the risk criterion is the broadest – it makes the article give due attention to the scope, context and purposes behind the processing. The second and third criteria are more specific – they concern the data processing’s frequency and character, and the nature of the data processed respectively.

As detailed in recital 94 of the GDPR, higher frequency processing leads to higher risk. It has been already established that, in the WP29 view, there exists a certain point of frequency of processing, which when surpassed leads the processing to be considered “non-occasional”. Combining these two viewpoints would imply, that once the frequency is at, or past, the point of frequency to be deemed occasional, the risk is too high for the derogation in 30(5) to be applicable.

The third criterion is simpler – one either processes sensitive data or one does not. Ignoring any problems with classifying data, the application is straightforward: sensitive data processing is too risky for the derogation in 30(5) to apply.

Based on the above, it can be concluded that failing either the second or third criteria is enough to also fail the first, risk-based, criterion. There is now a complete statement, which is “If the processing is too frequent, or if it concerns sensitive data, then it is likely to pose a risk for the data subject’s rights”. This is a logical statement, that can be simplified into a conditional statement: “if frequent or sensitive, then not safe”.

As a logical conditional statement, it should be possible to infer a contrapositive statement. While this may sound confusing, it is actually quite simple. Let us use the phrase “All dogs are mammals” as an example. The phrase can be rephrased into a conditional statement: “If something is a dog, then it is a mammal”. This conditional statement can be used to infer a contrapositive statement: “If something is not a mammal, then it is not a dog”.

Let us return to 30(5) and the conditional statement: “if frequent or sensitive, then not safe”. The contrapositive statement would be: “if safe, then not frequent or sensitive”. Putting that statement as a complete sentence: if the data processing is not likely to pose a risk for the data subject’s rights, then the processing is occasional, and not concerning sensitive data. Let us now examine this new statement closer.

Firstly, this does not seem to create any inconsistencies when it comes to the data nature criterion. It is logical that safe processing would not concern the sensitive categories of data.

However, when it comes to the frequency criterion, the statement runs into problems. The model falls apart if one were to imagine a frequent, but harmless, data processing activity. According to the model, any processing which is unlikely to create risk, must also be, to at least some degree, infrequent.

This may initially not seem to be an insurmountable problem. Perhaps it is simply so that frequent processing per definition cannot be harmless? However, such absolute argumentation would, as per its nature, be disproven by the existence of even a single instance of harmless, but frequent, processing. Considering possible measures that make the processing safer, such as the data subject' consent, the processing only concerning data of trivial nature, and a strict access policy, it seems increasingly implausible that there could not be a single instance of harmless, but frequent, processing. It is therefore this thesis' view that it must not be impossible for frequent processing to be unlikely to pose a risk for the data subject's rights.

So, there is a logical inconsistency in the model, which is therefore faulty. How can the model be fixed?

Earlier, it was established that the purpose of the frequency criterion in 30(5) is to guide in the risk assessment by looking at the legislator's opinion on the effects of increased frequency in recital 94 of the GDPR. What if that was not the case?

If the purpose of the frequency criterion in 30(5) is not to guide in the risk assessment, there must be some other logic behind its inclusion. Briefly thinking back on the WP29's position paper on 30(5), they framed their discussion on the meaning occasional in the light of the record-keeping's function in proper data management. This is a possible alternative logic for the criterions inclusion: the criterion exists to make sure firms cannot use the derogation in 30(5) to avoid examining their use of personal data. By keeping records of the data being processed frequently, the firm would gain the knowledge to adhere to the rest of the GDPR. The derogation in 30(5) was meant from the beginning, by the legislator, to be used as an opportunity for teaching SMEs.

This fixes the logical inconsistency in the model. By removing the relationship between the frequency criterion and the risk assessment, the criterion regarding "occasional" is now unrelated to the risk posed by the processing, and is instead related to what the legislator feels firms need to work on to achieve GDPR compliance.

What this interpretation means, is that the criteria for the derogation in 30(5) to apply have two purposes: the first is to confirm that the processing is safe, at least to a certain degree. The second, unrelated to the first, is to guide firms in their path to GDPR compliance, by ensuring that firms will always have to keep records about their commonly used processing. The WP29's focus on occasional processing, rather than the risk-assessment, in their position paper can be said to fall perfectly in line with this reasoning – 30(5) was meant, from the beginning, to have two, separate, tests.

However, there are other ways to fix the model's logical inconsistency. One of these solutions will now be examined closer, which concerns the WP29's interpretation of the character of "occasional"

2.1.3 An alternate interpretation

Occasional – as well as the French *occasionnel* – has the meaning: of being in relation to an occasion. Instead of being a signifier for the action repeating itself within intervals, the meaning, under such an interpretation, is to highlight the close connection to a happening or incident. In other words, the processing is related to something that is rarer than the norm.

As was discussed earlier, the WP29's interpretation of occasional has aspects concerning both character and frequency. What if the latter was removed from the definition – if occasional was only related to the character – context – of the processing? This solves the problems with the model, since the frequency aspect is removed altogether. However, the new definition of "occasional" needs to be described clearly, as to make sure no new problems are created.

The groundwork has been laid by the WP29 in their working paper 262. On a closer reading, the WP29 showcases some ambivalence on the total equation of occasional and non-repetitive – perhaps hinting at doubt. If the terms are clearly divided, so that "occasional" is solely related to character and "not repetitive" is solely related to frequency, the conclusion is that "occasional" is processing that happens outside of the regular course of action, as well as outside of a stable relationship.

By this definition, non-occasional processing would be directly connected to an enterprise's core. Employee workhours, labour performed, and daily correspondence would be examples of such processing. Interestingly enough, occasional processing could, under this definition, still be processing that would naturally flow from the enterprise's work, but be rare enough to not feature as a part of the day-to-day routine.

This will initially seem like an extremely broad definition that will often contain both sensitive and generally dangerous data processing – and that is correct. Such an interpretation means that the criterion regarding the processing not being occasional is much more unlikely to hinder the applicability of 30(5); the focus will instead be on the risk-assessment criteria. In fact, under this interpretation of "occasional", the occasional criterion becomes a part of the general risk-assessment. Much like the criterion regarding the processed data's nature, the occasional criterion becomes a check if the processing is a day-to-day regularity – both of these criteria are relatively binary checks for factors that serve as a red flag for a risk level over the accepted. The general risk-assessment test of the GDPR is to contain due consideration of the "nature, scope, context and purposes of processing" – the second and third criteria of 30(5) now tie directly together with this test when it comes to context and nature respectively. The somewhat opaque term of "occasional" is both made clearer, and made secondary to the legally certain concept of overall risk posed by the processing.

To put this in the structure of 30(5), processing that is a day-to-day occurrence, or that concerns sensitive data, is always at least likely to risk the rights and freedoms of the data subject. The logic model of 30(5) becomes: if day-to-day or sensitive, then not safe. The contrapositive of the model is then: if safe, then not day-to-day or sensitive. In other words, if the data processing is safe, at least to a degree, then it is neither done as a regular day-to-day operation in the enterprise, nor concerning sensitive data. Under this interpretation, it can therefore say that all of the criteria in 30(5) are part of a risk-assessment test, and that this does not lead to any logical inconsistencies or errors.

Let us now examine how these interpretations of "occasional" and "not repetitive" affect the rest of the GDPR.

2.1.4 Recital 111, 113 and derogations for specific situations

The WP29's guideline on the derogation in 30(5) interprets the meaning of occasional processing based on the use of the word in recital 111 of the GPDR – which's subject matter is data transfers. Equating data processing and data transferring is problematic for multiple reasons.

Firstly, it ignores the context. While article 3 of the GDPR, in theory, guarantees that the protection offered to data subjects is not affected by the physical location of the processing, in practice, enforcement outside of EU territory will never be as secure as the enforcement inside. Thus, the extensive ruleset on specifically data transfers – they are recognised as a source of risk.

Secondly, by equating "occasional" and "non-repetitive", the WP29 becomes unable to harmonize recital 111, 113 and article 49 with each other.

Recital 111 states that "Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim". According to the WP29, the recital, the requirement that the transfer is "occasional and necessary", is to be applied to 49(1) (b), (c), and (e).

Recital 113 concerns "transfers which can be qualified as not repetitive" but that "should be possible only in residual cases where none of the other grounds for transfer are applicable". In other words, the recital describes a measure that is to be seen as the last option for data transferring, a last resort. The corresponding text in the legalisation itself for this recital is found in article 49(1)(2).

Now, it should be noted, that the mention of "not-repetitive" was carried from recital 113 to 49(1)(2). Additionally, the requirement that the transferring is "necessary" was carried from both recital 111 and 113 into the respective clauses. "Occasional" however, is not found at all in the text of article 49.

As was discussed earlier, "occasional" as defined in working paper 262, has aspects concerning both the processing's character and frequency. A processing's character can be defined as its context; the parties involved. 49(1) (b), (c), and (e) have strong similarities regarding context: they concern contracts and legal claims. Based on the WP29 view, these transfers would have to happen outside

of a stable relationship to qualify as occasional. Why was this not stated directly in the text of article 49?

The answer is that the requirements of the processing, based on the processing's character, is implicit in the relationship between article 44, 46 and 49. Article 44 states that "All provisions in this Chapter [on data transfers] shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined". Article 46 details the various ways appropriate safeguards can be used when data is transferred in a stable relationship. Lastly, article 49 makes it clear that it is the last resort, containing derogations for specific situations that shall only be considered after considering other grounds for transfer. This is also the view that the WP29 and EDPB themselves advocate.[30]

The requirement in recital 111, that the transferring based on 49(1) (b), (c), and (e) is to be occasional, therefore becomes superfluous, as any stable relationship between two parties where the data transferring is a core characteristic, would make the whole of article 49 non-applicable – such transfers would have to be justified by article 46. Stating that the derogations in article 49 are only applicable to occasional processing would therefore be needless repetition.

However, under the WP29 view of "occasional", the word also has aspect concerning frequency of processing – or in this case, transferring. This is a requirement that is not found anywhere in the relationship between the articles on data transfer. It is therefore quite odd that the word "occasional" is not included in article 49, as it – in the WP29 view – constitutes an additional requirement to be fulfilled.

Under the alternate interpretation of occasional, presented above under the discussion on 30(5), the word only defines processing's character, or context. Under such an interpretation, there is nothing strange about the absence of the word in article 49, as the requirement is already implicit.

Returning to article 49(1)(2), where the term used is "not repetitive". Under the alternate interpretation of "occasional", the frequency aspect that was split is instead given solely to the term "not repetitive" – since this confers an additional requirement than the one implicit in article 49, the term's inclusion in both recital and article is logical.

To the WP29 interpretation's favour, where "occasional" and "not repetitive" have the same meaning, the paragraph has the same logical meaning in that case as well – save for the needless repetition of the non-stable relationship requirement mentioned earlier.

[30] See the following quote from "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679": "Hence, data exporters should first endeavour possibilities to frame the transfer with one of the mechanisms included in Articles 45 and 46 GDPR, and only in their absence use the derogations provided in Article 49 (1)", page 4.

2.1.5 The derogation from designating a representative

The last article where "occasional" is used is article 27, on representation from a non-EU processor or controller. The components of 27(2) (a) are highly similar to 30(5), but the wording and order differs. In 30(5), the criteria are in the order: general risk-assessment, occasional processing and sensitive data. In 27(2) (a), the order is occasional processing, sensitive data, and general risk-assessment. Additionally, sensitive data only precludes the derogation from being applicable if the processing is "large-scale", and the general risk-assessment now clarifies its components: "nature, scope, context and purposes of processing".

Especially interesting here is how the criterion regarding sensitive data changed. In their working paper 262, the WP29 subtly equated "occasional" with processing done on a smaller scale.[31] If this was the intended interpretation, "large-scale" processing of sensitive data being specified seems curios; would not the fact that the processing is occasional make this specification superfluous?

Secondly, recall the discussion earlier on 30(5) and its translation into a logic chain. 27(2) (a) has the same problem as 30(5): if "occasional" has a frequency aspect, then the reason for the criterion regarding occasional processing being included must be something else than to guide in the risk assessment. In 30(5), the reason was as a guiding measure in teaching firms GDPR adherence. In 27(2) (a), that explanation leaves something to be desired – designating a representative is a measure meant to enhance cooperation with DPAs and easier rights enforcement for the data subjects, but it does not guide the firm to GDPR compliance. The representative is responsible for all data processing, not just the non-occasional. As opposed to 30(5), 27(2) (a) is "all-or-nothing" – there is no separation of the different processing activities done by a single actor. Compare this to if the term "occasional" is kept free from any meaning regarding frequency, and instead only concerns the processing's characteristics: in that case, the logic chain of 27(2) (a) works fine.

Article 30(5) is the most definitive example of the attention paid to the special needs of SME – it is therefore not just an article, but also an indicator for how SMEs are to be treated. The proposed alternate interpretation of "occasional" leads to article 30(5) becoming more useful for SMEs, as it is more concrete and easier to incorporate into a simple corporate structure, but it also does this without decreasing the protection and respect afforded to the data subjects. Importantly, it is also compatible with the rest of the GDPR – perhaps even more so than the WP29's interpretation.

However, it does this by placing greater focus on assessment of general risk posed by a specific data processing action. Thus, while the test can lead to greater legal certainty, it requires that the question of how far a specific data processing action infringes upon the fundamental rights of data subjects. So, while the alternate interpretation of "occasional" in 30(5) leads to greater legal certainty, and diminishes the impact the GDPR has on SME's freedom to conduct

[31] See the last paragraph of page 11 in "Guidelines on Article 49 of Regulation 2016/679".

a business, it cannot be used until the question of proper balance between business and privacy interests can be answered. This problem will be returned to later.

Moving on, article 30(5) is not the only article pertaining to SMEs. As has been stated, but deserves to be restated: [1] the legislator intends for there to be special consideration paid to SME in the application of the GPDR, and [2] choose to, aside from the derogation in 30(5), to let this intent take form in the two articles corresponding to codes of conduct and certification respectively.

2.2 Articles on codes of conduct and certification

Regarding codes of conduct, article 40(1) states that:

> *The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.*

On the topic of certification, article 42(1) reads:

> *The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.*

While the phrasing differs, both articles effectively state that member states, DPA, the EDPB and the Commission shall encourage the development of codes of conduct/certification, and while doing this they shall take the specific needs of SME into account; it would seem apt if this in practice meant that they are to encourage codes of conduct/certification that meet the specific SME needs. Additionally, the above articles are supplemented by articles concerning supervisory bodies, more specifically article 41 concerning codes of conduct and article 43 concerning certification.

There will now be a brief overview of the combined functioning of both tools according to these articles.

Codes of conduct are to be sector-specific tools that lead an adhering firm to proper application of the GDPR. Each code is to have an independent monitoring body, an organisation or group that monitors code compliance. Codes are to be approved by the relevant DPA – if the code is related to processing activities in multiple member states, then it may, after passing through the EDPB, be approved as having EU-wide validity by the Commission.

Based purely on the text of the GDPR, certification initially may seem very similar to codes of conduct. They promote proper GDPR adherence, and are to have a supervisory body. However, while codes aim to promote general good practice within a relatively large and loosely defined area, certifications are focused entirely on the data processing itself. In other words, certification makes sure that a specific data processing action within the firm is GDPR compliant, while codes of conduct aim to promote general good practice.

The difference between the two is showcased in certification's ability to showcase compliance with article 25 "Data Protection by Design and Default", something a code of conduct cannot do. However, there are multiple instances in the GDPR where a code or a certification can showcase compliance. Article 25 is in fact the single instance where only certification suffices.

The two tools often blend together – a possible question is to which degree the average data subject will know, much less care, about the difference between code adherence and certification, and what this means for the signalling effects. Such discussions do however go outside the scope of this thesis, and will likely be possible to address in practice later.

At this point, a purely black letter interpretation of the GDPR articles has reached the end of its road. The thesis will therefore supplement it, partly by looking at the functioning of codes of conduct in the context of the old directive, and partly by looking at certification as it is currently used outside of strictly a GDPR context.

3. Self-regulation in the field of data protection

While certification is new to the GDPR, codes already existed in the old DPD. Described in article 27 of the directive, codes of conduct should "be intended to contribute to the proper implementation of [provisions pursuant to the Directive]"; the article also briefly described the adoption process before either national authorities or the WP29.

In 2003 the Commission, in their First Implementation Report, articulated a certain frustration about the lack of interest in EU-wide codes of conduct.[32] A 2009 report by Rand Europe presented two main factors: the non-functioning cooperation between DPA and firms, as well as a lack of resources in the DPA to review and validate and promote codes of conduct among firms.[33]

In 2009, there were two EU-wide codes of conduct, made by the International Air Transport Association, IATA, and the Federation of European Direct Marketing, FEDMA, respectively.[34] Eight years later in 2017, those two codes were still the

[32] See "First report on the implementation of the Data Protection Directive (95/46/EC)", page 26.
[33] See "Review of the European Data Protection Directive", RAND Europe, page 37.
[34] Ibid.

only EU-wide approved codes.[35] In comparison to the above, the number of national codes is staggering. The DPA in Berlin alone has been consulted on more successful codes than the WP29.[36]

The WP29 published a short working paper on codes of conduct back in 1998.[37] The following passage describes how the WP29 would evaluate submitted codes:

> *[determining whether or not a submitted code of conduct] is of sufficient quality and internal consistency and provide sufficient added value to the directives and other applicable data protection legislation, specifically whether the draft code is sufficiently focussed on the specific data protection questions and problems in the organisation or sector to which it is intended to apply and offers sufficiently clear solutions for these questions and problems.*[38]

While this may give the impression that codes of conduct need to be elaborate projects, in practice they may not be quite so grand. Above it was stated that the Federation of European Direct Marketing, FEDMA, had written one of the two cross-national codes of conduct approved by the WP29. The FEDMA code is composed out of seven chapters, concerning: [1] applicable law, [2] obtaining personal data, [3] responsibilities of the data controller, [4] dealing with data subjects' requests, [5] "Preference Services Systems", [6] transfers of data to non-EU countries, and [7] compliance and monitoring.[39]

Some of these chapters are relatively extensive, such as the chapter regarding the collection of personal data – other are short, such as the chapter on data transfers. The focus here is on giving concrete examples of good practice in specific situations, and rephrasing parts of the directive into every-day language; e.g. the data subject's rights regarding disclosure in the context of telemarketing.[40] The final chapter on monitoring compliance is noteworthy, as this was not a requirement for codes of conduct in the old Data Protection Directive.

Moving on, there is an abundance of different kinds of certification for data security: the ISO 27k/29100 family, COBIT, SSAE and PCI DSS are only a few. In the interest of keeping the scope somewhat tight, the ISO standards as well as SSAE 16, aka SOC 2 will be examined.

Both the 27k family and the 29100 family are not compromised out of a single document, but rather a collection of several different documents. These are

---

[35] See "Data Protection codes of conduct hitting the fast lane under GDPR", Bristows LLP, page 5.
[36] Ibid.
[37] "Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct".
[38] Ibid, page 4.
[39]"European Code of Practice for the Use of Personal Data in Direct Marketing".
[40] Ibid, page 7-8.

grouped into three categories: a management structure, a risk management system and a control system.[41]

Some of the main documents of the ISO 27k family are 27001, 27002 and 27005. These go from general documents, meant to give a general introduction at a top manager level – which would hopefully trickle down – to specific guidance on the data security aspects of individual firm measures such as the hiring process.[42]

The aim is to provide the "security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties".[43] While personal data would in some cases fall under this definition, calling it an "asset" does rhyme a bit funny with some of the fundamental GDPR principles, which see personal data as something belonging to the data subject.

The ISO 29100 family approaches personal data, or rather "personally identifiable information", PII, protection, in a way sometimes quite similar to the Union legislation. Actors are divided into controllers and processors;[44] many of the principles behind the text, such as data minimisation, collection limitation, consent and choice, are shared, and the way data is tied to a person is also quite close to the EU model.

It shares a number of aspects, and even some whole documents of the 27k family are directly referenced in the 29100 related documents.[45]

The ISOs are international standards, with multiple certifying bodies; while the standard itself is constant, the bodies responsible for the actual certifying are not tied to any specific auditing processes. When a legal entity wants to obtain certification under an ISO standard, they can, depending on the auditing organisation, expect some guidance from the organisation. The major part of the work: developing, implementing, and ensuring the effectiveness, as well as the continued effectiveness of the chosen measures is however up to the certification standard-seeking firm itself. The certifying body's task is closer to reviewing the enterprise's work in reaching the standard.[46]

The SSAE 16, aka SOC 2, is not a certification per se. It is rather a tool that allows an independent auditor to compare a declaration made by the enterprise regarding its intended practices to the independent auditor's impression of the enterprise's actual practices. The strengths of the SSAE 16 are the different variations the auditor's report can take; a type 1 report focuses on the enterprise's processing on a given day, while a type 2 report details the enterprise's

[41] "List of standards in the ISO 27000 family".
[42] Ibid.
[43] "ISO/IEC 27000 family - Information security management systems".
[44] "International Standard ISO/IEC 29100, First edition 2011-12-15"
[45] Ibid.
[46] See "Understanding data processors' ISO and SOC 2 credentials for GDPR compliance", Timothy Dickens, IAPP.

processing over a minimum period of 6 months.[47] However, the wealth of report variations also mean that a lot is asked of the enterprise in terms of time and effort to both request the correct type of report, and to properly understand the final statement.

3.1 Effectiveness of already existing codes and certification

With the matter examining the definition and function of codes and certification concluded, the question of how codes of conduct and certification – or at least their current form – meet the specific SME needs can be approached.

Even with the intent to only briefly cover the subject of privacy-centric certification, the above section did at times get relatively technical. That is a fact that is hard to avoid, since that character is almost integral to the current form of certification. The question is how realistic attaining an ISO certification is for smaller firms – especially micro sized firms will be left out in the cold due to the lack of guidance. Strong practical experience from the issuing organisations may alleviate this, by directing the enterprise's efforts towards the most critical areas, but that is hard to predict at this stage.

Furthermore, it is unclear if the ISO certifications actually respect the fundamental values of privacy. The lack of privacy focus in existing certification was in fact noted by the EDPB themselves in the guidelines on certification released in March of 2018;[48] the GDPR is overall highly critical of a "box-checking" mentality that does not incorporate personal data protection into the fundamental structure of a firm's processing – this is sadly something that seems prevalent in the 29100 family. This may partly be the effect of lack of development resources; the number of 29100 family of standards issued is so small that the ISO did not list it in their 2017 survey data about issued certifications.[49]

The SSAE 16 has many of the same basic strengths and weaknesses as the ISO standards. A firm that already has come most of the way in their work towards GDPR compliance may find the detailed report invaluable to cover blind spots – but a firm that has trouble getting started will most likely be overwhelmed.

Codes of conducts, on the other hand, are much simpler but also less flexible. The FEDMA code serves as a good indicator of what the WP29 meant when they asked for "sufficient quality and added value". Enterprises acting within the field that an accepted code caters to would most likely be able to quickly make progress in their GPDR adherence thanks to the specificity of examples and descriptions of common data processing.

However, codes also have less economic incentive behind them, which is crucial especially for the matter of supervision. Certification offers greater capabilities for both monetisation, due to the tailor-made service provided, as well as

[47] Ibid.

[48] "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679".

[49] See "ISO Survey 2017".

supervision – both during the initial certification as well as the annual renewals. Codes of conduct, on the other hand, often do not have the same contact between the code issuer and the code adherer. The FEDMA code simply states that "Companies should regularly monitor their compliance to this code (for example, via self-audits)".[50] Since the supervisory organisation needs to have enough insight to suspend and exclude enterprises that do not properly adhere to the code, or risk losing their status, code of conducts under the GDPR need a new structure compared to the old codes. While codes of conduct may be advantageous for SMEs, they therefore cannot be expected to be implemented within the short-term.

Additionally, much of the practical "added value" of codes of conduct is found in their practicality. In the words of the WP29, codes of conduct are to be applicable to "specific data protection questions and problems in the organisation or sector to which it is intended to apply" and offer "sufficiently clear solutions for these questions and problems".[51] This means that anyone that tries to write a modern code of conduct will run into the problem of trying to to provide an answer to the question of how far a specific data processing action infringes upon the fundamental rights of data subjects, which, as the WP29 themselves noted, is integral to creating a code of conduct of sufficient quality.

Regarding the question of codes of conduct, the fact that so few cross-border codes were ever approved is worrying. While codes of conduct were a far successful system on the national level, the author would like to point out that there was a switch from a directive to a regulation; the question of uniform application is now at the forefront. The GDPR makes the process of creating a cross-national code an extended part of the creation of a national code, as opposed to under the directive which simply presented the option;[52] the question of accountability and supervision would however perhaps lead to the organisation submitting the code trying to artificially limit the territorial scope of the submitted code. Still, the question remains of whether national codes of conduct are compatible with the GDPR's objective of preventing divergences from hampering the free movement of personal data within the internal market.[53]

The current problems with certification and codes of conduct are far from insurmountable. However, as the problems with both systems is connected to their economic viability, either for the issuing organisation or the applying organisation, there is a substantial risk that the systems will take a while to get rolling. If there, perhaps due to political pressure, are attempts to speed this process up, there is a risk that data protection offered by certification, or the independence of the organisation issuing codes of conduct, is lowered in an effort to decrease

[50] See "European Code of Practice for the Use of Personal Data in Direct Marketing", page 17.
[51] See "Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct", page 4.
[52] Compare the wording of article 40(7) to (10) of the GDPR to article 27(3) of the directive.
[53] See recital 13 of the GDPR.

running costs. The DPA need to have a long-term mindset to allow for functional self-regulation to form.

While the above is speculation, there is precedent for the fear that privacy protecting systems can be hollowed out due to economic pressure and legal pragmatism. While the matter needs some introduction, it is important for establishing the common denominators between the case and the current situation with SMEs, even if the system examined concerns firms several orders of magnitude bigger.

3.2 Binding corporate rules and legal pragmatism

Binding corporate rules, BCRs, were created to address a specific problem in the practical implementation of the DPD implementing national legislation. Around the turn of the century, compliance with EU data protection legislation, in matters of multi-national data transferring was done by: [1] incorporating EU Standard Contractual Clauses in all relevant contracts between all the concerned actors, and [2] meeting all formal permit and notification requirements in these Member States. This was cumbersome, expensive, slow, hard to incorporate into the firm's structure or management, and did often not lead to actual protection of any data subject's rights.[54]

First created back in 2003 in the WP29's working paper 74, BCRs were initially a type of code of conduct.[55] In 2008, the WP29 released three working papers, 153 to 155, providing guidance on the structure, requirements and key issues of successful BCR. They were finally codified in the GDPR under article 47.

Relatively few firms have gone through the whole BCR process; as off May 2018, a total of 130 firms had passed through the procedures.[56]

Their main purpose is to ensure adequate data protection in the case of data transfer from one branch of the company, located in the EU, to another, non-EU, actor within the same firm. Since EU data legislation has always worked towards real protection of EU citizens' rights, BCRs are, as the name implies, legally binding rules within the company which ensure that the firm will provide the same level of data protection for data processed outside the EU as for data processed within the EU.

BCRs also serve as the de facto showcase of data protection compliance for big firms; a prerequisite to showcasing that one has EU-level data protection globally within the firm, is to first have an adequate level of data protection within the EU.

---

[54] See "Binding corporate rules: corporate self-regulation of global data transfers", page 1-2.

[55] See "Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers: WP 74", page 6.

[56] See "List of companies for which the EU BCR cooperation procedure is closed Updated on 24 May 2018".

In October of 2015, the CJEU published their judgment in the *Schrems*[57] case, and with that declared the Safe Harbour agreement invalid. The agreement had, up until that point, served as a guarantee that the ensured level of data protection in the US would be adequate for safeguarding the rights and freedoms of EU citizens, thereby enabling the transfer of data from the EU to the US without any further safeguards.[58]

The case, simplified, was determined on the basis of the lack of EU equivalent rights in the US. The court noted that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter".[59]

With this decision, BCR were made highly relevant for all firms transferring data across the Atlantic – if the general level of data protection was not deemed adequate, then firms simply had to individually ensure that their data processing would not put EU citizens' rights and freedoms at risk. The WP29 was highly aware of this in their statement released soon after the ruling.[60] BCRs therefore allowed business to proceed as usual – with the stringent and extensive application procedure for BCRs, that did most likely lead to a higher level of data protection than under the Safe Harbour agreement.

However, there was and is an elephant in the room. In the EU, as seen in cases such as *Digital Rights Ireland*[61] and *Tele2*[62], general data surveillance is against the principles of the European Charter of Human Rights.[63] This is not strictly the case in the USA, as brought to public attention in the events surrounding WikiLeaks; American companies are obliged to cooperate with government authorities by giving access to the user's personal data.[64]

The current question is therefore whether US law obligating companies to share personal data with intelligence services is in conflict with the fundamental rights of the EU Charter – specifically with individuals' rights to an effective remedy; this is the question posed to the CJEU in a case which is currently pending: *Schrems 2.0*.[65]

---

[57] Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.
[58] See "New EU privacy rules could widen the policy gap with America", The Economist.
[59] Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 95.
[60] "Statement of the Article 29 Working Party on the Consequences of the Schrems Judgement" (sic).
[61] Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.
[62] Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.
[63] See Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 125; Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 65-68.
[64] See "US wants Twitter details of Wikileaks activists", BBC News.
[65] Case in progress as of 12 February 2019, *Facebook Ireland and Schrems*, C-311/18.

Independent of the court's final decision, there is merit in the view that BCRs have ultimately ended up in a spot where they are the legal justification for cross-Atlantic data transfers, but without truly answering the questions posed in *Schrems*.

While the work the corporations in question undertake to obtain the BCR approval must have some effect on the corporate culture and general awareness of data protection, it still is a far cry from the GDPR's ideal of giving real control to the data subjects. While BCRs may have led to greater legal certainty for corporations, it has happened at the expense of real proof that those corporations are committed to the protection of privacy and personal data.

Overturning the current system of BCRs would effectively cripple cross-Atlantic trade, without actually leading to better data protection in practice. This is as the actual problem is a vastly different view on data protection as a fundamental right across the EU and US.[66] The only way to solve that will be long-term measures where each step will have to be accepted by both the Union and the United States. It will be a long time before anyone can truly say "Mission Accomplished".

Returning to the central question of this thesis – defining how the specific situation and needs of SMEs should be incorporated into the GDPR – it has been established that codes of conduct, as well as certification has a long way to go before the systems can be called functional, especially in relationship to SMEs. However, by examining BCRs, it is clear that a system that is functional for corporate side is not the end all of proper data protection.

This thesis argues, that to take account of the specific situation and needs of SMEs, that these firms need to be provided legal certainty in the form of more specific requirements and obligations. However, it is vital for this to be done in a way that gives proper consideration the rights and interests of data subjects – partly to not undermine the GDPR's objectives and partly to ensure that the specific requirements and obligations provided will not suddenly change; in other words, to make sure that the legal certainty given is true.

BCRs were developed as a response to the combined failures of standard contract clauses. There failures were of undue cost and overt cumbersomeness for the firms, but also a lack of actual protection for data subjects – not entirely different than the current situation for SMEs.

However, after *Schrems*, when BCRs were further developed as a way to provide legal certainty to firms transferring data, the development was not shaped in accordance with the proper respect for the rights and interests of data subjects, as there were no real changes meant to alleviate the problems that were observed by the court in *Schrems*.

[66] See "Privacy Revisited – A Global Perspective on the Right to be Left Alone" page 36-37 and 171-172 for a brief overview.

This has ultimately resulted in the current situation, where the system as it is used today is pending to be considered before the CJEU in *Schrems 2.0*. Regardless of the court's ultimate judgment, the very fact that the case arrived at the CJEU at all is a source of sizeable legal uncertainty.

In other words, while there is a need for pragmatism when it comes to finding practical solutions to specific data protection questions and problems, it must always proceed with the proper balance between the interests of business and the interests of data subjects in mind. In this thesis' introductory chapter, it was stated that these both of these conflicting interests have a strong fundamental rights aspect. In the following section, case law of the CJEU will be examined in search for answers to the problems noted in the thesis so far.

4. Guidance from the courts

As briefly touch upon in the thesis' introductory chapter, the CJEU has given a broad definition of measures that limit the freedom to conduct a business. In *LIDL*[67], regarding an obligation concerning labelling, the court stated that such an obligation was:

> *liable to limit the exercise of that freedom to conduct a business, since such an obligation constrains its addressee in a manner which restricts the free use of the resources at his disposal because it obliges him to take measures which may represent a significant cost for him and have a considerable impact on the organisation of his activities*[68]

It is simple to see how the obligations laid down in the GDPR fall under this definition. Enterprises that handle the personal data of EU citizens therefore are subject to multiple infringement on the freedom to conduct a business, as per article 16 of the Charter.

This is of special importance to SME, which may have simple, straightforward organizational structures – in these cases, to fulfil the GPDR requirements can "represent a significant cost for him and have a considerable impact on the organization". However, these measures are of course created to safeguard the rights of the data subjects under articles 7 and 8 of the Charter; there therefore is a conflict of fundamental rights. In *Promusicae*[69] the court determined that, where there is conflict between fundamental rights, a proportionate compromise between all of them is to be found.

Historically speaking, in *Lindqvist*[70] the court stated that that the Data Protection Directive itself did not infringe upon the right to free speech, and it was up to the national authorities and courts to find the right compromise between the

[67] Judgment of 30 June 2016, *Lidl*, C-134/15, ECLI:EU:C:2016:498.
[68] Judgment of 30 June 2016, *Lidl*, C-134/15, ECLI:EU:C:2016:498, paragraph 29.
[69] Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54.
[70] Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

fundamental rights of data protection and rights infringed upon by the data protecting measures.

With the switch to a regulation, it is now up to Union authorities and the CJEU to find this compromise. While the current case law is not enough to give definitive general answers to how the interests of business and data subjects should be balanced, there are many cases in tangentially related areas.

It is the writer of this thesis' belief that it is possible, through looking at the case law of the Luxembourg, and various national courts, arrive at answers to two questions: one regarding the substance of privacy and business rights, and one regarding the makings of a standardised test for proportionality between the aforementioned rights.

The following subsection will examine the substance of the concerned rights; the examined case law will be judgments where the court made statements regarding the essence or core qualities of the infringed interests. Afterwards, another subsection will examine how these interests are to be balanced against each other; the examined cases will be judgments where the court discussed the merits of alternate measures, appropriate expectations, or general appropriateness of measures.

4.1 The substance of the concerned rights

Google Spain[71] concerned whether a natural individual had a right for certain search results on his name to be removed from the famous online search engine Google. The advocate general explicitly mentioned article 16 of the Charter in his opinion – in his view, the conflict stood between the privacy interests, in article 7 and 8 of the Charter, and the business interests, article 16, as well as the availability of information in an open society and free speech, as per article 11. The court, however, did not mention article 16 of the Charter, and instead simply referred to the "economic interest" of the firm, in this case the search engine operator Google.

The court, assessing the potential seriousness of the privacy infringement, found that the economic interest of Google could not alone balance out the conflict; the AG agreed in principle, stating that "especially [...] freedom of expression and freedom of information"[72] are of greater importance in the counterbalance in this case.

While some legal analysts have chosen to read this case as a general precedent, applicable to any conflict between business and privacy interests, the wording of the case does not mesh with this interpretation. In paragraph 97 of the judgment, the court states that privacy rights "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data

[71] Judgment of 13 May 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317.
[72] AG Jääskinen, 25 June 2013, *Google Spain*, C-131/12, ECLI:EU:C:2013:424, paragraph 128.

subject's name".[73] The court's wording makes it clear that the fact that the case concerned a search engine was vital for the court's argument. In other words, the search engine threatened the essence and substance of the privacy rights. This raises questions regarding what the substance of the privacy rights is, and how to define it.

Deutsches Weintor[74] and *Société Neptune*[75] are cases where the CJEU made it clear that infringements upon fundamental rights happen on a spectrum. In the cases, it was stated that legislation that controls the packaging and marketing of products can infringe upon the freedom to conduct business, but it does not infringe upon their core qualities, or the substance of the right. The rights of other, that the legislation seeks to protect, do therefore not need to be as threatened for the measures to still be found proportionate.

In *Google Spain* there is a strong example of an infringement upon the privacy rights that did concern the substance of the fundamental freedoms. What would be examples of measures that would be seen as infringements that do not concern the substance of the privacy rights?

Certain guidance can be found in *Schrems* in the form of a negative definition. While the case was examined earlier in this thesis in the context of data transfers, the case is also notable for containing guidance on the nature of the substance of the privacy rights: "public authorities [having] access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life".[76]

Moving on, the *Manni*[77] case will be examined. The case concerned a natural individual, who sought to erase his name from the Public Registry of Companies. The individual, Mr. Manni, was allegedly losing business as possible clients were informed by the Public Register that he had been the administrator of a company that was declared bankrupt 10 years before the main proceedings in the case.

The court's judgment was that the individual had no right to erasure – the disclosed personal data was limited, and justified by the legitimate purpose it served. The interference with the individual's privacy interests was therefore not disproportionate. The court also noted that, with the expiration of a sufficiently long period of time, limiting the access to the registry would perhaps be justified; the ten-year period in the case was however not long enough. The court stated that "in view of the range of possible scenarios [...] it seems impossible, at present, to identify a single time limit".[78]

---

[73] Judgment of 13 May 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317, paragraph 97.
[74] Judgment of 6 September 2012, *Deutsches Weintor*, C-544/10, ECLI:EU:C:2012:526.
[75] Judgment of 17 December 2015, *Société Neptune*, C-157/14, ECLI:EU:C:2015:823.
[76] Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 94.
[77] Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197.
[78] Ibid, paragraph 55.

Two things are of special note in the case. Firstly, the fact that "only for a limited number of personal data items" concerning "identity and the respective functions of persons having the power to bind the company" were required to be disclosed seemed to be a big contributor to the court finding the infringement upon Mr. Manni's rights proportionate.[79] Secondly, having stated that the infringements in the case were proportional, that removing or limiting access to the register entries could in a case-by-case assessment be "exceptionally justified, on compelling legitimate grounds relating to their particular situation"[80], particularly concerning cases where a sufficiently long period of time had passed.

The above cases, read together, make it clear that the substance of the privacy rights is threatened when the personal data kept fall under many different categories of classification, is collected and accessed for general, non-specific, reasons and kept for a long time relative to the reason for collection.

These points would roughly correspond to the principles of data minimisation, purpose limitation and storage limitation, respectively; all found in article 5 of the GDPR. According to the CJEU case law, data processing that respects these principles would therefore not threaten the substance of the privacy rights. Furthermore, data processing that naturally does not infringe upon these principles would also not threaten the substance of the privacy rights.

Now, let us return to the line of thought regarding businesses seen in *Deutsches Weintor* and *Société Neptune*. To repeat, in both of these cases, the substance of the right to conduct a business was not threatened by controls of advertising claims on packaging. It is therefore the opposite question than the one regarding the essence of privacy that now needs to be answered: What would be examples of measures that do concern the substance of the right to conduct a business?

In *Mc Fadden*[81], an enterprise was providing access to an open wi-fi network, which could be used to illegally download IP material. The CJEU examined three different measures, proposed by the asking court, for protecting the IP rights. The two first alternatives concerned filtering measures, and the termination of the network respectively. They were found to be non-proportionate in comparison to the enterprise's interests. The third alternative, protecting its open WI-FI network with a password, was found to be a proportionate measure to safeguard IP rights. Importantly, it did "not damage the essence of the right to freedom to conduct [the] business", as it consisted of only "marginally adjusting one of the technical options open to the provider in exercising its activity".[82]

The court noted that the intent was to create a need for identification to use the network service – while these measures do create some inconvenience for the firm, it could be argued that the IP rights can still relatively easily be infringed upon. What was the reason behind the court finding such a weak measure to be

[79] Ibid, paragraph 58.
[80] Ibid, paragraph 64.
[81] Judgment of 15 September 2016, *Mc Fadden*, C-484/14, ECLI:EU:C:2016:689.
[82] Ibid, paragraph 91.

proportionate? A possible explanation was the small scale of the enterprise providing the wi-fi network – in this case, more extensive and costly measures would simply put have been too intrusive in the emprise's economic interests. This is of especial importance as Mc Fadden's business consisted of selling and leasing lighting and sound systems. The wi-fi network was not integral to the core of the business – but forced termination would have gone against the substance of article 16. This is clearly in line with *LIDL*, and with defining the right of business as "the free use of the resources at [the business'] disposal".

However, that is not to say that the right to conduct a business enjoys wide protection. In *LIDL*, the court also stated that "the freedom to conduct a business is not absolute, but must be viewed in relation to its social function" and that "the freedom to conduct a business may be subject to a broad range of interventions on the part of public authorities which may limit the exercise of economic activity in the public interest".[83]

This can be seen clearly in *Sky Österreich*[84], where in the interest of promoting media pluralism, legislation that allowed an enterprise to only demand enough payment for a service to cover the cost of providing the service itself was found to be proportionate. Providing the service meant that the business had to aid its competitors – the real, total cost of providing the service would be higher than the cost of providing the service itself, leading to an overall loss for the enterprise. In this case, the public interest clearly weighed much heavier than the business interests in its free use of owned resources.

The core of the right to conduct a business is therefore quite elusive. While there exists a right to the free use of the resources at the business' disposal and measures which may represent a significant cost and have a considerable impact on the business' organisation are seen as infringements, it is also clear that such measures can clearly be accepted for the sake of somewhat nebulous concepts such as the public interest. A clear definition of the essence of article 16 is therefore not possible at the current time – it is however enough, to get started on a general test for proportionality.

4.2 A general test for proportionality

Legal certainty is a core concept of the rule of law – this is a statement so obvious that it borders on tautology. The GDPR proclaims its intent to provide "legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises".[85] The GDPR therefore aims to provide clear and precise rules, so that economic operators know what their rights and obligations are and can act accordingly.

This last point is the most important. All enterprises, not only SME, should be able to know what is expected of them. They should be able to, after examining

[83] Judgment of 30 June 2016, *Lidl*, C-134/15, ECLI:EU:C:2016:498, paragraph 30.
[84] Judgment of 22 January 2013, *Sky Österreich*, C-283/11, ECLI:EU:C:2013:28.
[85] Recital 13 of the GDPR.

their business, to deploy measures that protect the rights of their data subjects thereby securing their obligations as data controllers or processors. Furthermore, they should also know enough of their rights to be able to perform these measures within economic viability. In other words, economic operators should be able to determine the proper balance between the involved rights.

In *Volker und Markus Schecke and Eifert*[86], the AG, regarding the question of proportionality, said:

> *[on whether a measure is proportionate] Answering that final question involves specifying with clarity and precision exactly what the aim of the contested measures is, examining whether the specific measures chosen (with the particular degree of interference with rights that they entail) are appropriate to achieve that aim and checking that they do not go beyond what is necessary to do so.*[87]

In other words, to determine proportionality, there needs to be clarity regarding the aim of the contested measure – this is to be able to effectively answer the question of whether the measure is appropriate and necessary.

While this may appear simple, it is in practice quite complicated. There are some cases were the court simply states certain measures to be nonproportional. The sister cases of *Scarlet Extended*[88] and *SABAM*[89] are examples of such; in which filtering – a constant system which would check all data passing through the enterprise's service and remove content infringing upon IP rights – was found to be too intrusive a measure, both in terms of cost and administration, to safeguard IP rights. The cases are very similar – the court used the same reasoning, even lifting wording directly from the older case into the newer, despite the defendants in *Scarlet Extended* and *SABAM* being two different types of organisations: an internet service provider, ISP, and a social networking website respectively. The guidance here is simple: filtering, or in the words of the court: a "complicated, costly, permanent computer system at its own expense" is too intrusive.[90] That is of limited use in situations where other, less intrusive measures are discussed.

Volker und Markus Schecke and Eifert is a case where the court voluntarily proposed a number of possibly less intrusive measures. The case concerned publishing the names of companies benefiting from state funding – on other words, the principle of privacy was to be balanced against the interests of transparency.

---

[86] Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, ECLI:EU:C:2010:662.
[87] AG Sharpston, 17 June 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, ECLI:EU:C:2010:353, paragraph 87.
[88] Judgment of 24 November 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:771.
[89] Judgment of 16 February 2012, *SABAM*, C-360/10, ECLI:EU:C:2012:85.
[90] Judgment of 24 November 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:771, paragraph 48; Judgment of 16 February 2012, *SABAM*, C-360/10, ECLI:EU:C:2012:85, paragraph 46.

Regarding the less intrusive measures, the court noted that "limiting the publication of data by name relating to those beneficiaries according to the periods for which they received aid, or the frequency or nature and amount of aid received"[91] should have been considered. This echoes the previous discussion on the essence of the privacy rights – the court was proposing alternate measures for carrying out the same purpose, but that would collide less with the core of the rights of data subjects.

Secondly, another important thing to note in the case, is that the CJEU ultimately made a distinction only between the data of legal and natural individuals. However, before reaching that point, they had first divided the data into three different distinctions: data concerning natural persons, data concerning legal individuals that revealed information about natural persons, and data concerning only legal individuals – the second category would include, e.g., companies named after their owner. The reason for eventually dropping the second category was that "the obligation on the competent national authorities to examine, before the data in question are published and for each legal person which is a beneficiary of EAGF or EAFRD aid, whether the name of that person identifies natural persons would impose on those authorities an unreasonable administrative burden".[92] This does not concern business rights, as the statement concerns national authorities, but it does carry substantial similarities to the discussion from *LIDL*, concerning significant cost and impact on the organisation of business. The court clearly realised that some work must be allowed to be routine, and that economic viability must be kept in mind – even if, in this case, the actors acting against the data subjects were national authorities and not enterprises.

The CJEU has also commented on how different measures meant to protect the same interest interact in *ABNA*[93]. The case concerned the competing interest of public health – a subject where the EU gives itself discretion so broad that only a measure that is manifestly inappropriate in relation to the objective pursued is deemed unlawful.[94]

In this case, the provision in question required manufacturers of compound animal fodder to, at a customer's request, provide the composition of the fodder. The court stated that this requirement was unproportionate in regard to the objective of protecting public health.

The court came to this conclusion by stating that the provision had a serious impact on the economic interests of the manufacturing firms – the requirement did in effect mean that the value of any investment, research, or innovation on the subject of animal fodder was compromised, as the knowledge would be easily

[91] Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraph 81.
[92] Ibid, paragraph 87.
[93] Judgment of 6 December 2005, *ABNA*, C-453/03, C-11/04, C-12/04 and C-194/04, ECLI:EU:C:2005:741.
[94] See e.g. Judgment of 14 December 2004, *Swedish Match*, C-210/03, ECLI:EU:C:2004:802, paragraph 48.

obtainable by competitors. The positive effect the measure would have on public health could not justify this infringement; other existing measures would already allow both customers and relevant authorities to obtain enough information to make informed decisions and carry out their duties respectively. In other words, "doubling up" on protective measures is only proportional as far as those measures have additive effect.

This brings us to the closest the CJEU has given us to a proportionality test when it comes to business rights competing against other fundamental rights: the case of *Telekabel Wien*. Together with the previous discussion on the essence of the right to conduct a business, and privacy, as well as the preceding cases in this section, this is the makings of the standardised test spoken of earlier.

In *Telekabel Wien*[95], an internet service provider was required to implement measures having the effect of "making it difficult to achieve and of seriously discouraging"[96] infringements upon the IP rights of others. The court also gives an extensive line of thought on the possible actions by the enterprise.

> *First, an injunction such as that at issue in the main proceedings leaves its addressee to determine the specific measures to be taken in order to achieve the result sought, with the result that he can choose to put in place measures which are best adapted to the resources and abilities available to him and which are compatible with the other obligations and challenges which he will encounter in the exercise of his activity.*
>
> *Secondly, such an injunction allows its addressee to avoid liability by proving that he has taken all reasonable measures. That possibility of exoneration clearly has the effect that the addressee of the injunction will not be required to make unbearable sacrifices, which seems justified in particular in the light of the fact that he is not the author of the infringement of the fundamental right of intellectual property which has led to the adoption of the injunction.*[97]

The first paragraph concerns the enterprise's freedom to, after noticing an infringement upon one or more fundamental rights, choose a measure to alleviate that infringement that is appropriate both in terms of cost, as well as compatibility with the enterprise in question's management and actions. This also means, that to avoid limiting the businesses' right to freely use the resources at its disposal, businesses should not have the choice of appropriate measures made for them.

---

[95] Judgment of 27 March 2014, *Telekabel Wien*, C-314/12, ECLI:EU:C:2014:192.
[96] Ibid, paragraph 62-64.
[97] Ibid, paragraph 52-53.

The second paragraph makes it clear that the enterprise should be allowed to avoid liability, as long as it has taken all reasonable measures. The term "all reasonable measures" could possibly create problems together with the findings from *ABNA* – clearly it would be incompatible to claim that measures that infringe upon the right to conduct business must have real effect for them to not infringe too far upon the fundamental right, while also claiming that "all" measures must be taken. The combined term "all reasonable" must therefore limit the amount of required measures to a point where the effect of the stacked measures is diminishing. Furthermore, as was discussed above, that which can reasonably be expected from a firm is highly contingent on the firm's size and capability to affect the society and public around it. Terminating a non-vital wi-fi network was not reasonable in the case of *Mc Fadden*, but providing a service at an effective loss to competitors was reasonable in *Sky Österreich*. Certain measures are, as a general rule, considered reasonable or unreasonable: filtering was unreasonable in *Mc Fadden,* as well as *Scarlet Extended* and *SABAM*; provisions regarding marketing and packaging were reasonable in *Deutsches Weintor* and *Société Neptune*. In *Volker und Markus Schecke and Eifert*, examining each processed company individually for similarities between its name and its owner's name was considered literally "unreasonable".

In the latter part of the second paragraph, it is stated that "unbearable sacrifices" will not be required, which is justified especially in the light of the fact that the source of the infringements upon the fundamental right in question is not the party that will be financing and carrying out the measures. This sentence is interesting, as it concerns who the authored the infringing action. In the context of personal data processing, this will always be the processing enterprise – claiming that those enterprises should therefore always be required to make "unbearable sacrifices" is impractical at best. A more fitting definition would be if the infringement could have been avoided – certain processing will simply be required to carry out a business. The enterprise is then not the exclusive origin of this processing, and therefore infringement: rather the origin is the contractual agreement, between the data subject and the enterprise, itself. Greater sacrifices should, according to such a line of thought, instead be reserved for cases where the processing initiative is solely taken by the data processor. In the GDPR context, the origin of the intent to process data would be showcased in the chosen grounds for lawful processing in article 6: processing justified by 6(1)(b) would in most instances be an example of shared intent, while 6(1)(f) would represent processing based on the intent of the controller/processor.

In *Manni,* the court especially noted that it was "natural persons who choose to participate in trade through such a company"[98] that were required to disclose their data; thereby making it clear that the individual data subject's role and intent is not without consequence. Further guidance can be found in the CJEU case *L'Oréal*[99], where an operator of an online marketplace was required by injunction

[98] Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 59.
[99] Judgment of 12 July 2011, *L'Oréal*, C-324/09, ECLI:EU:C:2011:474.

to take measure in bringing an end to IP infringements that happened on the online marketplace; these measures were to be "effective, proportionate, dissuasive" and should "not create barriers to legitimate trade".[100] That which is of particular interest here is that the operator was not a mere conduit, i.e. passive party, to the infringements, as they had purchased certain advertising which aided the actors actively infringing upon the IP rights. The operator was therefore not "the author of the infringement", but clearly closer to that author than the ISP in the present case *Telekabel Wien*. When comparing the wording of the two cases, measures in *L'Oréal* were to be "effective and dissuasive" in bringing an end to the IP infringement, while the measures in *Telekabel Wien* were to be "seriously discouraging" against IP infringement, as well as making infringement "difficult to achieve".

In *Telekabel Wien*, which concerned an ISP's obligations in preventing IP infringements, the CJEU stated that "that they have the effect of preventing unauthorised access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users [who are breaching IP rights]".[101] Directly translating this allowed level of infringement upon the IP rights to a theoretical level of allowed infringement upon the privacy rights is most likely impossible, partly because the CJEU has never ranked the level of protection the fundamental rights deserve. However, as was discussed earlier, the substance of the right to privacy and the right to protection of personal data concerns data minimisation, purpose limitation, and storage limitation. It is therefore highly likely that any possible measures must at least acknowledge these three points to be considered reasonable.

This should all be understood as a decision more on general intent of measures, than any specific tools being preferred – not entirely unlike the technologically neutral approach of the GDPR. While still containing a number of questions, as is natural for these types of legal tools, formalising a test like this, along the lines of such tools as the Gebhard formula, would go a long way towards minimising legal uncertainty.

Telekabel Wien has already been used as supporting case law in cases regarding proportionality. An example of this is a case from a national court, more specifically the Irish Court of Appeals: *Sony Music Entertainment Ireland Ltd & Ors v UPC Communications Ireland Ltd*.[102] The facts of the case concerned a system that required ISP to, when receiving notices of copyright breaches from the rightsholders, send two notices to the customer behind the flagged IP address, before a termination of the service at the third instance of a copyright breach. The question posed was if this was to be in accordance with EU law, especially in terms of proportionality.

[100] Ibid, paragraph 144.
[101] Judgment of 27 March 2014, *Telekabel Wien*, C-314/12, ECLI:EU:C:2014:192, paragraph 62-64.
[102] Ireland / Court of Appeal / [2016] IECA 231

When discussing the appropriate cost-level and intrusiveness of measures, the judge looked at *Telekabel Wien*, *L'Oréal* and *Scarlet Extended* for guidance, and ultimately compressed the cases into a five-step test, which was used to evaluate the contentious measure and its associated costs. The final conclusion was that building a specialised computer system for a cost between 800 000 and 960 000 Euro was neither unnecessarily complicated nor costly in the light of the gross turnover of the ISP being approximately 340 million Euro.

Let us now finally structure this case law into a something more concrete: a possible test for evaluating the proportionality of a privacy protection measure under the GDPR. As was explained in the beginning of the thesis, the eventual creation of such a test will be paramount of both the SME's specific needs and situation.

The case law has touched upon three points, which the test needs to consider: the data processing's nature, the infringement on privacy by the processing and the infringement on the right to conduct a business by the data protection measures.

First, drawing primarily from the second point of the examined quote from *Telekabel Wien*, together with *Manni* and *L'Oréal*, is the question of the source of the intent behind the processing. The origin of the data processing is it found in the combined will of the data subject and controller/processor? Or is it solely for the benefit of the latter? Sorting these kinds of processing from the onset is useful for a variety of reasons. In case of a common will behind the processing, there is likely both greater understanding and involvement from the data subject. Additionally, the test allows the enterprises that do the bare minimum of data processing to be considered on their merits – many SMEs that perform traditional and basic services will likely fall into this group, as those kinds of non-technical enterprise do not require, or even draw benefit, from more extensive data processing.

The second step would incorporate the case law regarding the essence of the privacy rights, such as *Google Spain, Manni, Volker und Markus Schecke and Eifert* and *Schrems*. It would involve examining the processing and determining in turn whether it respects purpose minimisation, data minimisation and storage limitation. This could either be the case by special care and revision from the data controller or processor, or because the data processing by nature does not extend past what is needed.

The third and final step would determine what the impact of additional protection would have on the enterprise's organisation, as well as the costs of those measures. Something that is of decisive importance here is the focus on the concerned specific enterprise – as was established after examining the case law regarding the essence of the freedom to conduct a business, enterprises are judged based on their societal function and the public interest; *Mc Fadden* could be read as a sign that SMEs are judged quite kindly in this regard. On the other hand *Sky Österreich*, make it clear that larger, more disruptive enterprises have more asked out of them. Additionally, the possible added measures would have

to be evaluated on their possible effectiveness. As was determined in *ABNA*, multiple measures that aim to provide the same type of protection would be allowed until a certain point of diminishing returns.

The proposed test, as follows, would be applied to proposed data protection measures to determine whether they would be proportional:

i. Is the origin of data processing found in the common will of the parties?
ii. Is the data processing compliant with purpose minimisation, data minimisation and storage limitation?
iii. While taking the principles of necessity and diminishing returns in account, as well as the answers to the two questions above: are the proposed data protection measures appropriate in terms of cost and impact on the enterprise's organisation?

The two initial questions are therefore meant to guide in determining the character and gravity of data processing, and to influence the final decision taken in question number three. While the test cannot be the sole tool used to evaluate a conflict – it notably does not factor in any other involved fundamental rights – it serves as an indicator for how the CJEU could use their existing case law to create a strong foundation for future discussion on the matter of personal data protection, and thereby make the GDPR's commitment to legal certainty in recital 13 that much more meaningful. More specifically, this test can also be used to determine the appropriateness of individual measures, as well as guide in the general risk assessment of a specific data processing action. As was established in the thesis' introductory chapter, both of these features are instrumental in alleviating s the problems posed by SMEs' specific situation.

However, the CJEU has shown themselves to be set on a course that is not entirely set on lightening the load on SMEs' shoulders. In addition to the cases looked at above, the CJEU has also judged a number of cases with more direct relevance for the application of specific parts of the then relevant data protection legislation. Examining this material in detail would be material for a completely different text. There is however one case that has such a strong connection to this thesis' central focus – SMEs – that it deserves the attention. That case is *Wirtschaftsakademie.* [103]

In the case, a German firm was found to be a joint data controller together with Facebook for the data collected by the German firm's fan page. The judgment makes no mention of the firm's status as an SME; as of January 2019, the firm states on its website that it currently employs 386 employees.[104] So, while there is little doubt that the firm is not a SME, there is however a clear difference in power between the enterprise and Facebook – a power imbalance situation that SMEs will often find themselves in.

[103] Judgment of 5 June 2018, *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388.
[104] "Die Wirtschaftsakademie Schleswig-Holstein im Überblick" (company website's "About Us" page).

Namely, the court did not delve deeper into the question of whether the German firm could have fulfilled their data protection duties while using the ready-made service provided by Facebook. While the court stated that joint control did not mean joint liability, it did not provide any guidance on how the liability should be divided. It is the lack of elaboration on the relationship between these parties that is problematic. In practice there may be substantial power imbalances between cooperating actors – an example would be the case in question. Depending on the contractual clauses between the parties – which will be formed entirely to the larger actor's advantage – smaller actors may run into a complicated web of liability. Smaller actors often use the services of corporations such as Google and Facebook to interact with customers, advertise, perform basic data tracking and other tools they lack the resources to do themselves; there is considerable risk that smaller firms may in practice be locked out of these useful resources without clearer rules on how liability is to be divided.

In cases such as *Nowak*[105], in which the court was asked for guidance regarding the definition of personal data, the CJEU predicted the follow-up questions, regarding the limits of the supplied definition, and answered them. While it is ultimately a question of discretion, the court in *Nowak* recognised the principle that law must be made with its practical consequences in mind, and therefore went beyond the question posed to the court. A similar approach in *Wirtschaftsakademie* would have resulted in much less legal uncertainty for SMEs and weaker contractual parties in general.

What is truly worrying is that the CJEU's ruling in *Wirtschaftsakademie* bears resemblance to the more business-unfriendly guidelines published by the WP29, such as working paper 169.

In working paper 169, the WP29 states that "the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law". The WP29 states, in an example, that contractual terms being "take it or leave it" does not impact the smaller party's duties when it comes to data protection, and that if there is a "lack of availability in the market of other suitable providers", then smaller party should contact "competent authorities, such as DPAs, consumer protection and antitrust authorities, etc.". The WP29 does not state what the smaller party should do until a suitable provider is available.[106]

This begs the question: does both the CJEU and the WP29 truly expect firms to abstain from a valuable service – a service most likely widely used by the firm's competitors?

This section on case law has been spent examining the possible road to greater legal certainty, and how that theoretical solution would respect and balance the rights of the involved parties. This last section has begun to take us to another

[105] Judgment of 20 December 2017, *Nowak*, C-434/16, ECLI:EU:C:2017:994.
[106] See "Opinion 1/2010 on the concepts of "controller" and "processor"", page 26.

question: how is the balance of interests right now? As the reader may have suspected – especially after reading the preceding paragraph – it is the author's belief that SMEs are currently experiencing an encroachment upon their right to conduct a business.

The end of this thesis is close. The current situation will now be examined, and evaluated based on the provided consideration for SMEs, and how it fares in terms of balance of interests.

5. Possible courses of action and conclusion

The current outlook for the humble SME in the realm of data protection is bleak. Early investigative reports have shown that SMEs in general are having problems with adoption – the maturity of their GDPR compliance is behind larger firms', while also taking a large toll on the SMEs' resources.[107] Statistical papers have found that EU ventures have seen their investment fall in comparison to their US counterparts. The GDPR's effect was particularly pronounced for ventures up to three years old, where an average reduction of 19% in the number of deals was observed.[108] While pre-GDPR discussion often brought up the point of the positive effect GDPR compliance would have on customer relations, research has shown that privacy seals and marks are underdeveloped and misunderstood by the public. Test participants placed higher value on symbols they recognised, even if the symbol's significance in the current example was low, and generally had problems evaluating the actual meaning of supplied information.[109]

The CJEU's ruling in *Wirtschaftsakademie* was just examined: delivered in June of 2018, it is a "hot of the presses" insight into the court's thinking in regards of data protection. If this is combined with an EDPB that releases more market-unfriendly guidance, such as that exhibited in working paper 169, or more recently in the WP29's views on article 30(5), then it is hard to see a road to quick recovery.

While this thesis presented an alternate interpretation of article 30(5) that would be more in line with the specific needs and situation of SMEs, as well as infringing less upon the freedom to conduct a business, all the while not diminishing the protection offered to data subjects when needed, that interpretation was built on the principle of general risk-assessment, which is currently tricky to implement.

While the legislator hopes that codes of conduct and certification will help SMEs deal with the new law, was shown that both systems are currently not up to the task. Certification is unsuitable for the specific situation of SMEs, which is characterised by a lack of management tools and specialist knowledge. Furthermore,

[107] See "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)", Sirur, S., Nurse, J. R. C. and Webb, H., page 88-89 and 94-95.
[108] See "The Short-Run Effects of GDPR on Technology Venture Investment", Jia, J., Jin, G., Zhe and Wagman, L., page 17.
[109] See "How Website Trust Seals Nurture Bad Browsing Habits", George Paliy.

the current available standards examined are lacking in regard to supervision and accountability. Codes of conduct are better suited for SMEs, but they have similar deficiencies when it comes to supervision and accountability. Additionally, cross-border codes of conduct are currently almost non-existent. With the switch from the old directive to a regulation with the GDPR, the continued viability of national codes of conduct is questionable.

The directive was in force for almost twenty years, and no more than two cross-border codes of conduct were approved. Getting a code of conduct to pass through the approval process under the GDPR will be more difficult than under the directive, due to the new requirements notably regarding oversight and accountability. This is troublesome, as codes of conduct could otherwise serve as a general foundation for firms to get started on their GDPR adherence. Certification, while a highly useful tool for firms that are looking for ways to finalise, evaluate and review their data processing, is not catered to firms that struggle to even begin their journey towards GDPR compliance.

This thesis noted that codes of conduct's quality were based on their ability to provide sufficiently clear solutions for questions and problems facing data processing firms. It would therefore be vital for code's ability to provide "added value", which the WP29 themselves emphasis the weight of, that it is possible to give an answer on the appropriateness of individual data protection measures.

What should be done to alleviate these problems?

In the section on case law, the following test was presented as a possible combination of the CJEU's current case law on the freedom to conduct a business and the privacy rights:

i. Is the origin of data processing found in the common will of the parties?
ii. Is the data processing compliant with purpose minimisation, data minimisation and storage limitation?
iii. While taking the principle of diminishing returns in account, as well as the answers to the two questions above: are the current data protection measures in the upper limit of what can be done without undue cost and impact on the enterprise's organisation?

This test serves both as a direct, specific solution to some of the problems which SMEs are facing due to their specific situation and needs, and as the foundation for future development. As stated in the thesis' introductory chapter, the benefits of this specific type of test are: [1] greater legal certainty to firms, and [2] safeguarding due consideration to both the freedom to conduct a business and the privacy interests.

For the benefits of specifically SMEs, the second point, on the balance between rights and interests, is particularly important, as it allows for special consideration to be paid to the specific SME situation. More specifically, it opens up the possibility to handle SMEs in way that infringes less upon their freedom to conduct business – which is, as was established in the introductory chapter,

threatened by the GDPR – while justifying this based on SMEs' lesser infringements onto their data subject's rights.

SMEs perform less data tracking and analysing, instead often processing data based on consent and contractual duties. As this means they infringe less upon the data subject's rights and interests, it is vital that this is noted – which the test does, in the first and second questions.

The third question goes further into the nature of the right to conduct a business – as noted, the freedom is not quite clear in the current case law. However, in cases such as *LIDL* and *Sky Österreich*, the CJEU has made it clear that the societal role of a firm is of importance when it comes to infringing upon its rights. While general statements of a type of firm's public importance are hard to give, if any type of firm can be said to have innate importance, it would most likely be SMEs.

By allowing a test for balancing the practical consequences for the involved rights and interests to serve as the basis for future development, the risk a of a repeat of the development history of BCRs is diminished. When all measures are judged on their merits and demerits in regard to both of the conflicting interests, structural weaknesses in the legal construction of the measure are detected early on in the process: thereby precluding the creation of high-volatility court cases such as *Schrems 2.0*.

However, for SMEs, the most important contribution of the test would be that of obtaining greater legal certainty regarding the appropriateness of specific data protection measures. As was stated in the thesis' introductory chapter, this would be vital for SMEs that lack the tools and knowledge to effectively transform the GDPR's principles into concrete actions to take – which brings us to the other benefit of the three-questions test.

The three-question test, or similar, will be instrumental in the development of codes of conduct. As the ability of the supervisory organisation to ascertain the appropriateness of individual measures as answers to specific questions and problems rises, so does their ability to provide truly useful and cost-saving material for organisations which the code caters to. With greater benefit for organisations comes greater interest, which could be turned to opportunities for monetisation – with added resources, the supervisory organisation could expand its activities, providing better guidance, and most importantly update the code as technology advances, thereby fulfilling the requirements of reviewing and updating data protection measures as necessary.

On the topic of expanded guidance, the supervisory organisation could eventually release guidelines on the average level of risk posed by specific processing done by an example firm – almost like a sector-wide data protection impact assessment. Enterprises could then compare their processing to this average, while

taking notice of mitigating or aggravating differences.[110] With the greater understanding of the general risk posed by specific processing, the alternate interpretation of 30(5) presented could become truly useful. The greater focus on posed risk would also incentivise SMEs to implement better data protection – as a rising level of data security would result in the record-keeping obligation diminishing. This would meet the specific needs of SME, be more in line with their specific situation's focus on day-to-day business and therefore infringing less upon the freedom to conduct a business, as well as not diminish the protection offered to data subjects. As the section regarding 30(5) made clear, the alternate interpretation of "occasional" that changes the meaning of 30(5) meshes with the rest of the GDPR and provides greater legal certainty; recall how AG Sharpston in *Volker und Markus Schecke and Eifert* stated that it should be possible to "with clarity and precision" state a rights infringing measure's aim.

A firm carrying out certain data processing actions could, with the help the three-question test, determine a number of possible data protection measures providing adequate protection. By then comparing these measures against each other, on the merits of cost and impact on the organisation's activities, the general infringement onto the freedom to conduct a business would decrease.

Additionally, this would make the long-term growth of SMEs smoother, as tools like DPOs and DPIAs would more easily be incorporated into a firm that had experience with the risk-based assessment from the beginning.

This is not to say the individual firms would be able to ignore incorporating data protection into their firm on a fundamental level – the test makes this clear by placing the data processing principles of purpose minimisation, data minimisation and storage limitation at the forefront.

In short, the three-question test would both lead to general benefits for SMEs, based on their simpler data processing based on consent or contractual necessity, as well as their combined value for the Union market, and more specific benefits by enabling the proper functioning of codes of conduct and the derogation from record-keeping in 30(5). Both parts of the test, concerning legal certainty and balance of rights and interests, can be used to give due consideration to the specific SME needs – most importantly, this can be done in a way that does not diminish the importance of any of the legislation's principles, and allows the GDPR to stay cohesive and logical.

With the three-question test providing a solid foundation for the legal development, the national DPA and EDPB can spend more time on the observed structural failings of the current proceedings.

On the subject of joint liability for data controllers, the EDPB can provide guidelines that – while safeguarding the principle of an accountable legal or natural individual for each data processing action – make sure that the current

[110] Compare this proposal to that of sector-wide DPO which Sergio Fumagalli argued for at the GDPR conference at Politecnico University, Milan.

landscape of services and out-sourcing is not unduly disrupted. While the CJEU made it clear in *Wirtschaftsakademie* that joint liability would not categorically mean equal liability, the authorities need to be mindful of how a power imbalance between the contractual parties can affect the division of costs. The stronger party may in their terms-of-use documents designate a main establishment purely on its merits to the own company, possibly leading to the weaker party being subject to regulation from "foreign" DPA. In the case of companies such as Facebook, which's business hinges on data processing, the stronger party may have little interest in giving the weaker service user the opportunity to not process data – in such cases, joint liability could in practice entail a possibility for the stronger party to offload liability onto the weaker service user.

While the practical development is yet to be seen, the point is that joint liability is a delicate question which will have long-running consequences. Many SMEs lack the manpower or expertise to handle delicate issues such as online payment procedures or data storage. Outsourcing these services is often a net gain for personal data protection, as the specialised actors can ensure a higher level of protection against hackers;[111] which is in the direct interest of data subjects. While the service provided in *Wirtschaftsakademie* was of a nature that could not be considered integral to the German firm's business, the court made it clear in *Mc Fadden* that the essence of the freedom to conduct a business can be threatened even if the contested service was not integral to the core of the business. While the authorities clearly hope that mounting pressure from service users will force bad actors to improve their data protection, the short-run effects may have considerable impact on the organisation of smaller firm's activities – directly infringing their right to conduct a business.

When making smaller firms liable for data processing they in practice cannot control or influence outside of the indirect power exercised by choosing their provider of the service, it is of paramount importance that there are a number of actors on the market that actually provide the service in such a way that the smaller enterprise can avoid liability. Giving SMEs a "Sophie's Choice" – a choice where all options are unbearable – risks leading to firms either seeing possible GDPR fines as a cost for doing business, or hampering their own business by avoiding outsourcing – even in cases where doing so would have led to greater data protection. The EDPB could avoid this by releasing guidelines for how liability would be shared between contractual partners.

The EDPB would also be the main catalysator for the development of cross-border codes of conduct. As the thesis has noted, cross-border codes of conduct will be important for preventing divergences from hampering the free movement of personal data within the internal market; similar actions as those taken, or not taken, by the WP29 during the years of the directive, which mainly created national codes, could create serious problems in regards of sunk costs. RAND Europe noted two points which contributed to this dearth of cross-national codes: non-functioning cooperation between DPA and firms, as well as a lack of

[111] See "The Evolving Role of SAAS and IT Outsourcing in SMB IT Security", page 4-6.

resources in the DPA to review and validate and promote codes of conduct among firms.

While the second point is not something the EDPB itself can change, there are signs that the EDPB are taking things in a new direction in regards of the first. The EDPB is currently building "on top" of existing certification, more specifically the ISO/IEC 17065/2012 on Requirements for bodies certifying products, processes and services, when it comes to accreditation of certification bodies under Article 43.[112] This is most likely the way to go in terms of speeding up the adaptation rate while keeping costs as low as possible; it is also likely to be more familiar to market actors than something completely new. The EDPB recently released new guidelines on codes of conduct for public consultation – while the document does not delve very deeply, it is nonetheless welcome as the old working paper on codes was from 1998.[113] What will be of truly vital importance is the further development.

Certification will more likely than not play some role GDPR self-regulation for SMEs, but in the short-term it will most likely be a lesser one. The main problem noted in regard of SME inappropriateness is the lack of compatibility with the specific situation of SMEs, more specifically their corporate structure; which is a problem there is no short-term solution for. Perhaps the omission of any mention of SMEs in recital 100 is a sign the legislator was aware of this.

While the issue of organisational supervision in regard to codes and certification is vexing, there is danger in waiting for a perfect solution, as the appetite for implementing costly data security may ebb away, together with the GDPR's existence in the public's awareness, as data scandals and breaches, perhaps due to oversaturation, disappear from headlines. If the supervisory organisations are to have full insight from the beginning, it is possible that neither codes nor certifications will ever take of; it is up to the EDPB and DPA to find the right balance together with market actors that allow for the self-regulatory systems to grow and develop.

The European Commission divides its policy in relation to SMEs into five priority areas, covering:

- the promotion of entrepreneurship and skills;
- the improvement of SMEs' access to markets;
- cutting red tape;
- the improvement of SMEs' growth potential, and;
- strengthening dialogue and consultation with SME stakeholders.[114]

---

[112] "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)".
[113] "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679"; Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct.
[114] See Eurostat - Structural Business Statistics - Small and medium-sized enterprises (SMEs).

Through this thesis, these areas have inadvertently been touched upon in various ways. It is plain to see that the EDPB cannot act without paying attention to the consequences of their guidelines and guidance. Article 70(4) of the GDPR states that the EDPB "shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period"; the author finds giving due attention to the "specific SME needs" nothing less than appropriate. However, it should also be recognized that the EDPB cannot give final answers on questions that ultimately belong at the CJEU – which is why the three-question test, or similar, is needed.

5.1 Conclusion

The GDPR's overall objective can be seen as promoting good practice in the field of data protection.

Bad practice is in many cases quite similar to good practice – in the vast majority of use cases, the outcome will be the same. It is in the edge cases that the corner-cutting and cost-saving of bad practice creates disasters like Cambridge Analytica. These outcomes were not intended by the system creators – there was no person at Facebook whose intent was to leak several millions of users' data. It is a bug, not a feature. While the GDPR can be overbearing and cumbersome, costly and complicated, those are also characteristics of the good practice it is promoting.

It bears to be repeated, that the decision to make the GDPR technology neutral, and thereby future-proof, is nothing less than ambitious. While the law can appear opaque and troublesome, it bears to be repeated that the GDPR is still in its early phases, and with future-proofing, the early phases are the most precarious.

However, that does not mean the authorities should simply sit and wait. If the reader would allow for a car analogy: begin motor braking early, and there is no need for a sudden deceleration later. If the authorities act now, when there is still incentive and awareness in the industry, there will be a smoother ride later. They need to show that data protection is not necessarily a zero-sum game, and that data subjects, firms, and investors can all draw benefits from the GDPR.

It is the author of this thesis' view that SMEs are as integral to a functioning GDPR as they are to the EU's economy. SMEs deserve legal certainty, and denying them this will lead to weaker protection of personal data, on top of far-reaching economic damage as both investment and innovation suffers.

In this thesis' introductory chapter, it was stated that the thesis' objective was to answer how Union authorities can incorporate the specific situation and needs of SME into the GDPR, while respecting the proper balance between the freedom to conduct a business and the respect for private and family life and protection of personal data.

The special situation of SMEs is characterised by a lack of management tools and a focus on day-to-day business; the GDPR compliance procedure of larger firms is not viable, as it requires resources that smaller firms simply do not have.

Additionally, the specific situation of SMEs also includes their relationship with contractual partners, and their ability to shape contracts that make them joint data controllers. Due to these challenges, the GDPR obligations risk infringing deeper into SMEs' freedom to conduct a business, in comparison to larger firms.

The specific needs of SMEs are measures to alleviate these problems. Out of the possible measures examined, the thesis noted that specifically article 30(5) and codes of conduct were of interest, but that both were currently severely hampered in their ability to meet the specific SME needs. More specifically, the way the derogation article 30(5) was interpreted by the EDPB narrowed its application to practical non-existence. Codes of conduct could not provide the clear solutions to specific problems which were the basis for their practical use.

The thesis also briefly examined the controversial self-regulatory system of BCRs to give context to the weight given to finding the proper balance between the involved rights and interests, as well as the recent developments in regards to shared liability when the data processing companies had larger power imbalances.

After examining relevant case law, a possible test for ascertaining the proper balance between the involved rights in the context of data protection measures was proposed. The three-question test could be used for determining the appropriateness of specific data protection measures in regard to specific data processing actions, and could also be used as a basis for determining the general risk level posed by a processing activity. This would enable the function of codes of conduct, and also make the use of an alternate interpretation of article 30(5), more in line with a SMEs' specific situation and needs, which was proposed earlier in the thesis, possible.

The thesis finally noted that while the creation of the three-question test or similar was up to the CJEU, the EDPB could improve the specific situation of SMEs by providing additional guidance on the topic of joint liability, which was recently complicated by the CJEU's ruling in *Wirtschaftsakademie,* as well as work together with market actors for the creation of successful cross-national codes of conduct.

If the views presented in this thesis are considered in future development, then it is the author's belief that SMEs will partly see their specific needs met by greater legal certainty, which will also aid in the development of codes of conduct to further alleviate the problems associated with SMEs' specific situation. The most important thing in the future work of national and Union actors is that the development happens in accordance with the privacy interests of the data subject, as to further both the data protection and the economic functioning of the EU.

Lastly, this thesis wants to make one last point regarding a basic legal concept: fairness. As has been discussed, the GDPR aims to bring order to an age of oversharing of personal data, securing the rights of individuals and reigning in scandal-ridden firms for the good of the market. However, that is only one view.

Another is that of sour grapes – that the GDPR is a way for Union legislators to knock down the national champions of the US, all while conveniently overlooking the misdeeds of smaller EU firms.[115] Without considering the merits of these arguments, it is clear that the proponents of the second argument will be working directly against those that favour the first; fairness, as well as the image of fairness, are therefore of paramount importance. It is important, not only for the economic health of the single market and the protection of EU citizens' personal data, that the legal certainty given to firms is equal – it is also for the sake of the Union's place in the world.

[115] See "The French fine against Google is the start of a war", The Economist.

Bibliography

Academic Journals and papers

Jackson, O. (2018) 'Many small firms are still unprepared for GDPR', *International Financial Law Review*, p. 1. Available at: http://www.iflr.com/Article/3791042/Many-small-firms-are-still-unprepared-for-GDPR.html

Jia, J., Jin, G., Zhe and Wagman, L. (2018) 'The Short-Run Effects of GDPR on Technology Venture Investment'. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912

Narayanan, A. and Shmatikov, V. (2009) 'De-anonymizing Social Networks'. Available at: https://arxiv.org/abs/0903.3276

Sirur, S., Nurse, J. R. C. and Webb, H. (2018) 'Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)'. Available at: https://arxiv.org/abs/1808.07338

Articles from Journalistic Media

"As GDPR nears, Google searches for privacy are at a 12-year high", The Economist, May 21 2018, accessed 8 February 2019.
Available at: https://www.economist.com/graphic-detail/2018/05/21/as-gdpr-nears-google-searches-for-privacy-are-at-a-12-year-high

Michael Kassner, "Anatomy of the Target data breach: Missed opportunities and lessons learned", ZDNet, Feb 2 2015, accessed 8 February 2019.
Available at: https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

"New EU privacy rules could widen the policy gap with America", The Economist, Oct 5 2015, accessed 8 February 2019.
Available at: https://www.economist.com/international/2015/10/05/new-eu-privacy-rules-could-widen-the-policy-gap-with-america

"The French fine against Google is the start of a war", The Economist, 24 Jan 2019, accessed 8 February 2019.
Available at: https://www.economist.com/business/2019/01/24/the-french-fine-against-google-is-the-start-of-a-war

"US wants Twitter details of Wikileaks activists", BBC News, Jan 8 2011, accessed 8 February 2019.
Available at: https://www.bbc.com/news/world-us-canada-12141530#share-tools

"Who will be the main loser from Europe's new data-privacy law?", The Economist, May 26 2018, accessed 8 February 2019.
Available at: https://www.economist.com/business/2018/05/26/who-will-be-the-main-loser-from-europes-new-data-privacy-law

Books

Krotoszynski, Ronald J. (2016). *Privacy Revisited A Global Perspective on the Right to Be Left Alone*. Oxford University Press

Moerel, E. M. L. (2012) *Binding corporate rules : corporate self-regulation of global data transfers*. Oxford : Oxford University Press, 2012.

Uddenberg, Anders (2015). *Growth in established SMEs: Exploring the innovative and ambitious firm*. Lic.-avh. Linköping : Linköpings universitet, 2015

Codes of conduct and Certification

EUROPEAN CODE OF PRACTICE FOR THE USE OF PERSONAL DATA IN DIRECT MARKETING, FEDMA, accessed 8 February 2019.
Available at: http://www.amd.pt/fedma.pdf

"INTERNATIONAL STANDARD ISO/IEC 29100 First edition 2011-12-15 Information technology — Security techniques — Privacy framework", accessed 8 February 2019.
Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en

"ISO/IEC 27000 family - Information security management systems", accessed 8 February 2019.
Available at: https://www.iso.org/isoiec-27001-information-security.html

"ISO Survey 2017", accessed 8 February 2019.
Available at: https://www.iso.org/the-iso-survey.html

List of standards in the ISO 27000 family, accessed 8 February 2019.
Available at:
https://www.iso.org/search.html?q=27000&hPP=10&idx=all_en&p=0&hFR[category][0]=standard

European Union

Article 29 Working Party (WP29)

Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct: WP13. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp13_en.pdf

Guidelines on Article 49 of Regulation 2016/679 WP 262. Available at:
http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846

List of companies for which the EU BCR cooperation procedure is closed, accessed 8 February 2019. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841

Opinion 1/2010 on the concepts of "controller" and "processor: WP 169. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

STATEMENT OF THE ARTICLE 29 WORKING PARTY ON THE CONSEQUENCES OF THE SCHREMS JUDGMENT. Available at: https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules: WP 155. Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=43738

Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers: WP 74. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

Working Document setting up a framework for the structure of Binding Corporate Rules: WP 154. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf

Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules: WP 153. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf

WORKING PARTY 29 POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR. Available at: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422

Commission

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises

First report on the implementation of the Data Protection Directive (95/46/EC)

ENISA

“Guidelines for SMEs on the security of personal data processing”, accessed 8 February 2019.
Available at: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Eurostat

Eurostat - Statistics on small and medium-sized enterprises, accessed 8 February 2019.
Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_small_and_medium-sized_enterprises#Country_by_country_analysis

Eurostat - Structural Business Statistics - Small and medium-sized enterprises (SMEs), accessed 8 February 2019.
Available at: https://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme?p_p_id=NavTreeportletprod_WAR_NavTreeportletprod_INSTANCE_vxlB58HY09rg&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-

Employment, Social Affairs & Inclusion

Guide for training in SMEs (2009). Luxembourg : Publications Office of the European Union, 2009. Available at: https://publications.europa.eu/en/publication-detail/-/publication/1020b85f-dcc4-4c80-8d6e-65f4617aa3cd

European Data Protection Board (EDPB)

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_1_2018_certification_en.pdf

Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679). Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_4_2018_accreditation_en.pdf

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

The European Data Protection Board Endorsement 1/2018. Available at: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents.pdf

Legislation

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) No 181/2011 of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

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

Material and Studies from independent organisations

“Data Protection codes of conduct hitting the fast lane under GDPR”, Bristows LLP, accessed 8 February 2019.
Available at: https://www.bristowscookiejar.com/trends/data-protection-codes-of-conduct-hitting-the-fast-lane-under-gdpr

George Paliy, “How Website Trust Seals Nurture Bad Browsing Habits”, accessed 8 February 2019.
Available at: https://stopad.io/blog/how-website-trust-seals-nurture-bad-browsing-habits

“GDPR Compliance Status A Comparison of US, UK and EU Companies”, TrustArc, accessed 8 February 2019.
Available at: https://info.trustarc.com/Web-Resource-2018-07-12-GDPR-ResearchReport_LP.html

Larry Hardesty, “How hard is it to 'de-anonymize' cellphone data?”, MIT News Office, accessed 8 February 2019.
Available at: http://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data

“Review of the European Data Protection Directive”, RAND Europe, accessed 8 February 2019.
Available at: https://www.rand.org/pubs/technical_reports/TR710.html

“Symantec Corporation Internet Security Threat Report 2013”, Symantec, accessed 8 February 2019.
Available at: https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

Timothy Dickens, “Understanding data processors’ ISO and SOC 2 credentials for GDPR compliance”, accessed 8 February 2019.
Available at: https://iapp.org/news/a/understanding-data-processors-iso-and-soc-2-credentials-for-gdpr-compliance/

“THE EVOLVING ROLE OF SAAS AND IT OUTSOURCINGIN SMB IT SECURITY”, Kaspersky Lab, accessed 8 February 2019.
Available at: https://media.kaspersky.com/en/business-security/evolving-role-of-saas-and-it-outsourcing-in-smb-it-security-report.pdf

“The Race to GDPR: A Study of Companies in the United States & Europe”, Ponemon Institute, accessed 8 February 2019.
Available at: https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf

Other

Datainspektionen “About Us” section of website, accessed 8 February 2019.
Available at: https://www.datainspektionen.se/om-oss/organisation/

Die Wirtschaftsakademie Schleswig-Holstein im Überblick, accessed 8 February 2019.
Available at: https://www.wak-sh.de/unternehmen/zahlen-fakten/

Summary of speech by Sergio Fumagalli held at GDPR conference at Politecnico University, Milan, accessed 8 February 2019.
Available at: https://europrivacy.info/2017/01/25/a-sustainable-and-effective-privacy-for-smes/

Table of Cases

CJEU

Judgments

Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596

Judgment of 14 December 2004, *Swedish Match*, C-210/03, ECLI:EU:C:2004:802

Judgment of 6 December 2005, *ABNA*, C-453/03, C-11/04, C-12/04 and C-194/04, ECLI:EU:C:2005:741

Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54

Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, ECLI:EU:C:2010:662

Judgment of 24 November 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:771

Judgment of 16 February 2012, *SABAM*, C-360/10, ECLI:EU:C:2012:85

Judgment of 6 September 2012, *Deutsches Weintor*, C-544/10, ECLI:EU:C:2012:526

Judgment of 22 January 2013, *Sky Österreich*, C-283/11, ECLI:EU:C:2013:28.

Judgment of 13 May 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317

Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, ECLI:EU:C:2014:238

Judgment of 27 March 2014, *Telekabel Wien*, C-314/12, ECLI:EU:C:2014:192

Judgment of 17 December 2015, *Société Neptune*, C-157/14, ECLI:EU:C:2015:823

Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650

Judgment of 15 September 2016, *Mc Fadden*, C-484/14, ECLI:EU:C:2016:689

Judgment of 30 June 2016, *Lidl*, C-134/15, ECLI:EU:C:2016:498.

Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:970

Judgment of 5 June 2018, *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388.

Judgment of 20 December 2017, *Nowak*, C-434/16, ECLI:EU:C:2017:994

Case in progress as of 12 February 2019, *Facebook Ireland and Schrems*, C-311/18.

Opinions

AG Sharpston, 17 June 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, ECLI:EU:C:2010:353

AG Jääskinen, 25 June 2013, *Google Spain*, C-131/12, ECLI:EU:C:2013:424

National courts

Ireland - Court of Appeal / [2016] IECA 231