Responsibility for Data Protection in a Networked World

On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe

by **René Mahieu, Joris van Hoboken and Hadi Asghari***

Abstract: In the current networked world, almost no system in which personal data is processed stands on its own. For example, websites and mobile applications integrate third party services for behavioral targeting, user analytics, navigation, and many other functionalities. Governments build central infrastructures to share data efficiently between different branches of government and with other organisations. This paper analyses the current system in Europe for determining who is (or better, are) responsible for observing data protection obligations in such networked service settings. In doing so we address the following problems: (1) of ambiguity in applying the concept of data controller in networked settings; and (2) of insufficiencies in the framework for establishing the extent of the responsibilities in situations of joint control. We look at how the law and regulators address these problems and how the European Court of Justice tackles these problems by applying the principle of "effective and complete protection". The issue of joint responsibility has gained particular relevance in the wake of Wirtschaftsakademie, a case recently decided by the European Court of Justice. In this case, a Facebook fan page administrator was found to be a joint-controller and therefore jointly responsible, together with Facebook, for observing data protection rules. Following this decision, there are many more situations of joint control than previously thought. As a consequence, part of the responsibility for compliance with data protection legislation and risk of enforcement measures are moved to those who integrate external services. This will change the incentive structure in such a way that joint-controllers will place a much higher value on data protection. To explore the practical implications of the legal framework, we analyse a number of examples taken from our earlier empirical work on the right of access to reflect on the newly emerging data responsibility infrastructure. We show that the coordination of responsibilities is complex in practice because many organisations do not have a clear overview of data flows, there are power imbalances between different actors, and personal data governance is often happening in separated specialised units.

Keywords: GDPR; data controller; joint-control; right of access; C-210/16 Wirtschaftsakademie; principle of "effective and complete protection"; access rights

Recommended citation: René Mahieu, Joris van Hoboken and Hadi Asghari, Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe, 10 (2019) JIPITEC 85 para 1.

A. Introduction

1 European data protection law grants individuals rights in relation to their personal data, such as the right to transparency and the right to request access, correction or erasure. Legally speaking, these rights are granted in relation to the organisations that are in charge of the processing of their data, vis-à-vis the so-called data controllers. Therefore, for the system of rights to function, it should be possible to determine who counts as the data controller for the processing of personal data in specific contexts. In the end, it is the data controller who has obligations towards the data subject. And it is towards the data controller that the data subjects exercise their rights.

2 As others have noted, the legal framework for determining responsibility under European data protection law - which has its roots in the 1960s - may not function well in the current socio-technical environment.[1] Nonetheless, the core of this framework was retained as the basis of the current General Data Protection Regulation (GDPR).[2] In two recent high profile cases, *Google Spain*[3] and *Wirtschaftsakademie,*[4] national courts asked the European Court of Justice (ECJ) questions regarding how the framework of responsibility allocation should be applied. In both cases the ECJ expands the concept of data controller, arguing that these broad interpretations are in line with the principle of "effective and complete protection", a principle first introduced by the Court in *Google Spain.*[5]

3 This paper analyses the current system for determining who is (or better, are) responsible for observing data protection obligations in networked service settings.[6] In doing so we address the following problems: (1) of ambiguity in applying the concept of data controller in networked settings; and (2) of insufficiencies in the framework for establishing the extent of the responsibilities in situations of joint control. Both the Article 29 Working Party (Working Party) and the GDPR address these problems but leave many questions unanswered. The ECJ has now tackled the issues by applying the principle of "effective and complete protection".

4 In section B. of this paper, in order to answer these questions, we analyse the relevant legal provisions of the Data Protection Directive (DPD) (95/46/EC) and the GDPR, the guidance of the Working Party,[7] and the recent ECJ judgment in the case *Wirtschaftsakademie*. We find that, following the interpretation of the Court regarding the concept of data controller in this case, many more actors in networked settings could be considered data controllers than was previously considered. We conclude that under the ECJ's interpretation, any actor who has a purpose for a data processing operation, and can directly influence that processing, can be considered a data controller. Moreover, we find that, notwithstanding

* By René Mahieu, doctoral candidate at Interdisciplinary Research Group on Law Science Technology & Society (LSTS) at Vrije Universiteit Brussel (VUB), connected to the Chair 'Fundamental Rights and the Digital Transformation'; Joris van Hoboken, chair 'Fundamental Rights and Digital Transformation' at Vrije Universiteit Brussel (VUB) and Senior Researcher at the Institute for Information Law (IViR) at the University of Amsterdam. The Chair at VUB is established at the Interdisciplinary Research Group on Law Science Technology & Society (LSTS), with the support of Microsoft; Hadi Asghari, assistant professor department Technology, Policy and Management (TPM) at Delft University of Technology.

1 See for example Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 Ohio State Law Journal 1217; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179.

2 Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) [2016] OJ L119/1.

3 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González* [2014] EU:C:2014:317.

4 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] EU:C:2018:388.

5 A search of the CURIA database shows that the "effective and complete protection" formulation was first used in *Google Spain* and since in the judgments on *Weltimmo*, *Schrems*, *Wirtschaftsakademie* and *Jehovan todistajat.*

6 There has been academic work on the responsibility in European data protection regulation in general (e.g. Brendan Van Alsenoy, 'Allocating Responsibility among Controllers, Processors, and "Everything in between": The Definition of Actors and Roles in Directive 95/46/EC' (2012) 28 Computer Law & Security Review 25.) and in specific cases such as intermediary publishers (David Erdos, 'Intermediary Publishers and European Data Protection: Delimiting the Ambit of Responsibility for Third-Party Rights through a Synthetic Interpretation of the EU Acquis' [2018] International Journal of Law and Information Technology 1.) such as hosting providers, search engines, blogging services and social media (Patrick Van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 Computer Law & Security Review 535.) on which this paper builds. However, the *Wirtschaftsakademie* judgement as well as the introduction of the GDPR merit a new look at the situation.

7 The Article 29 Working Party is an independent advisory body comprising of members from the national Data Protection Authorities, which writes opinions interpreting specific elements of data protection law. while these documents are not legally binding they do tend to have impact (Christoper Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007) , 9-10). To give an example of the influence of this opinion, see how it figures prominently in the decision of the Administrative Court of Schleswig and the opinion of Advocate General Bot on ECJ C-210/16 (2017).

the specific inclusion of a provision in the GDPR on the attribution of responsibility among joint controllers, it is still unclear what the legal consequences are in case the joint controllers do not suitably arrange their responsibility or fail to uphold the terms of the arrangement. In light of the Court's broad interpretation of the possibility of joint controllership, we conclude that these are urgent questions, that should be answered in future guidance of the European Data Protection Board (EDPB)[8] and future court decisions, such as *Fashion ID*.[9]

5 In section C., we analyse some of the practical implications of the current data responsibility infrastructure, with a focus on the right of access and transparency.[10] We do this by building on examples taken from our earlier empirical work on this topic. We show that the coordination of responsibilities is complex in practice because many organisations do not have a clear overview of data flows, there are power imbalances between different actors, and personal data governance is often happening in separated specialised units.

8 The EDPB replaced the Article 29 Working Party. It is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities.

9 *Fashion ID* deals with similar questions as *Wirtschaftsakadmie*, but this case is not yet decided by the Court. An opinion in this case has recently been delivered by Advocate General Bobek. See: *Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 26 January 2017 — Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV (C-40/17)* (ECJ). See B.III.2. and C.I for a further discussion of this case.

10 Previous work on the responsibility for data access rights has focused on the difficulty, from the perspective of the data subject, of determining who the data controller is. See Xavier Duncan L'Hoiry and Clive Norris, 'The Honest Data Protection Officer's Guide to Enable Citizens to Exercise Their Subject Access Rights: Lessons from a Ten-Country European Study' (2015) 5 International Data Privacy Law 190. This study on the exercise of data access rights shows how difficult it is for a data subject to find out who the data controller is and how much effort it takes to find the contact details of the data controller. Similarly, Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4. This paper reports on the amount of time and clicks it takes to find the privacy policy of data controllers. However, in these instances it is presupposed that, with regards to the data processing taking place, it is clear from the legal point of view, who the data controller is. And the problem presented is how the data subject can find and/or reach this data controller. However, there are numerous cases in which it is ambiguous who the data controller is, or who the right data controller is for a data subject to turn to in the case of a number of different networked data processing operations.

B. Data protection responsibility in networked settings: The Law

6 In the EU,[11] the development of the legal framework for determining responsibility for data protection in networked settings comes directly from the Data Protection Directive (DPD).[12] While the GDPR recently came into force, key elements for the determination of responsibility for data protection within the GDPR are therefore a continuity. Because of this, the analysis of the commentaries on this directive, as well as opinions by the Article 29 Working Party and legal literature, are still relevant and will be included in this section.

7 This section is organised as follows. We start with an analysis of the key concepts of the responsibility framework (data controller, data processor). In section B.II, we discuss three Article 29 Working Party opinions in which it develops a more detailed interpretation of the responsibility framework. These influential opinions gave more body to the basic concepts, and also focused on the application of the framework in networked settings. In section B.III, we will discuss a case recently decided by the ECJ, *Wirtschaftsakademie*, in which the Court came to a landmark decision with regards to the reach of the concept of data controller, and the criteria for joint control. In the last section (B.IV), we will discuss the changes brought by the GDPR. Specifically, we look if the open questions that were laid bare by the Court are resolved by its additional provisions on joint control.

I. Controller and processor

8 The two central actors whose relation is governed by data protection legislation are the data subject and the data controller. In addition to these two main actors, the European data protection framework includes data processors; actors which pursue operations on behalf of others (data controllers).

11 In this paper we restrict ourselves to an analysis of the EU law. Other data protection frameworks, such as for example Canada's PIPEDA, are quite different, for example because they do not have the explicit controller-processor distinction. It would be very interesting to conduct further research in order to investigate how such different frameworks fare with regards to the complicated issues we raise in this paper.

12 The genealogy of the key legal actors (data controller, data processor, data subject) can be traced back to the 1970s (See Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179, 184). However, its current formulation is very close to that in the DPD to such an extent that most of the legal interpretation can be applied to the GDPR.

9 Data controllers are responsible for compliance with the obligations following from data protection law including ensuring that data subjects can exercise their data subject rights. Article 24(1) GDPR gives them the responsibility to make sure that data processing is in accordance with the regulation and the articles 12 until 23 which cover the rights of the data subject are also directed at the controller. Moreover, data controllers are liable to pay compensation in case of unlawful processing leading to damage (art. 82 GDPR).[13] "Data controller" is defined in article 4(7) GDPR as follows: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".[14]

10 Data processors are secondary actors in data protection regulation. According to article 28 GDPR, they process data on behalf of the controller, and they are not allowed to process personal data except on the instructions of the controller.[15] Article 4(8) GDPR defines "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

11 These basic elements of the legal framework of the GDPR have been carried forward without substantial changes from the DPD, while they are difficult to apply to contemporary practices of personal data processing. The legal categories of data controller, data processor and data subject form what Tene (2013) has called a "linear model". It is a model that fits to an environment of centralised data processing with independent relationships between data subjects and data controllers, which was prevalent around the time that the DPD was written. Within this logic underlying the law, the controller is the main architect of an information system and decides the why and how of the system's operations. In building the system, the controller might use or integrate the systems and services of other organisations; but this happens under the controller's control and responsibility.[16] Several authors have noted that there are problems in applying this restricting dichotomy between data controller and data processor to the complex relationships between actors which characterise the contemporary technological and economic reality.[17] As a consequence, there are many situations in which it is unclear to what extent organisations have data protection obligations.

12 Gürses and van Hoboken (2017) have argued that recent developments in software production have major implications for data protection and privacy governance more generally. The shift from shrink-wrap software to software as a service, and the rise of the mobile internet, cloud computing and agile software development processes, have meant that the way in and the extent to which personal data is being processed across multiple actors has changed dramatically. Software is becoming more modular, meaning that most applications, websites and other software is built out of service modules of third-party software. Many of these modules are offered across organisational and sectoral boundaries and their quality and efficiency are contingent on the effective capture of personal data to function. These developments, in addition to data-driven monetisation strategies, will make it increasingly complex to apply the existing linear controller-processor model.

II. Article 29 Working Party guidance

13 The Article 29 Working Party provided guidance on how to apply the basic concepts of data protection law in its opinion *1/2010 on the concepts of "controller" and "processor"*. This was in reaction to "a lack of clarity of certain aspects of these concepts [of data controller and data processor]", and noting that "the concrete application of the concepts of data controller and data processor is becoming increasingly complex", in particular because of "the

13 Processors can also be liable but only if they did not comply with the instructions given to it by the controller (Article 82(2) GDPR). Article 23(1) DPD assigned liability for damages to data subject to the data controller.

14 This definition of data controller in the GDPR is almost identical to the formulation in the DPD where it is defined as follows in article 2(d): "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data".

15 The role of the processor is also discussed in Recital 81 GDPR. See similarly art.16 and art.17 DPD.

16 This framework can be compared to the situation where a contractor that uses subcontractors in the building of a house, keeps the final responsibility for the quality of the house, and the car manufacturer being responsible for the whole car even when much of the parts may be built by suppliers.

17 See Christoper Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007) 72; Brendan van Alsenoy, 'Allocating Responsibility among Controllers, Processors, and "Everything in between": The Definition of Actors and Roles in Directive 95/46/EC' (2012) 28 Computer Law & Security Review 25, 35; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179, 184.

increasing complexity of the environment".[18] The analytical framework developed in this opinion was subsequently applied in opinion 2/2010 to online behavioural advertising.[19] Both opinions touch on three key issues:

(1) Definition of controller: interprets the phrase "determines the purposes and means of processing" and introduces controller as a "functional concept"; and

(2) Joint controllership: develops a framework for determining whether two actors qualify as joint controllers; and

(3) Division of responsibility: discusses how the different responsibilities should be divided between joint controllers and to what extent they are liable.

14 We will see in the discussion of recent case law (in section B.III) that some elements of the opinions help to achieve a consistent application of data protection law as intended. However, there are also more problematic elements that have led and will likely continue to lead to considerable confusion, in particular with regards to determining who is responsible for upholding data protection obligations, as well as with regards to the extent of this responsibility.

1. Controller: determining the purposes and means

15 To clarify the concept of controller, the Working Party rephrases what it means to determine the purposes and means of processing into the one who determines the *"why"* and the *"how"* of the processing of personal data.[20]

16 About determining the *purposes,* the Working Party states: "one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions 'why is this processing taking place? Who initiated it?'"[21] For example, a building owner that asks a security company to install cameras in order to secure their building initiates the processing of personal data; they decide why processing takes place. Therefore, they are considered the controller.[22] The security company, even if it handles some of the personal data, is considered a data processor.

17 According to the Working Party "determination of the *means* [...] includes both technical and organizational questions where the decision can be well delegated to processors (e.g. 'which hardware and software shall be used?'), and essential elements which are traditionally and inherently reserved to the determination of the controller such as 'which data shall be processed?', 'for how long shall they be processed?', 'who shall have access to them?', and so on."[23]

18 The Working Party further deliberates the extent to which an entity must determine the purposes and means to be considered a controller. The question of why the processing is happening in the first place is essential: determining this purpose(s) unequivocally leads to the qualification as controller.[24] With regards to the question of how the processing is carried out, there is more flexibility, and "it is well possible that the technical and organizational means are determined exclusively by the data processor."[25] However, an entity or person who determines the "essential means" is considered a controller.[26] So while the wording of the law seems to imply that determining both the purposes and means of processing are required to be considered a controller, the Working Party asserts that there can be situations in which a processor decides on the non-essential means and the controller decides only on purposes. Moreover, an entity that decides on essential means is also a controller. Effectively, the question of determining the purposes *and* means is transformed into determining the purposes *or* the *essential* means.[27]

19 The factual circumstances, rather than what is written in a contract, are leading to establish who is the controller. "The concept is [...] functional in the sense that it is intended to allocate responsibilities

18 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 2.

19 See Frederik J Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International 2015) for a detailed work on data protection in the area of behavioral targeting. Borgesius does not discuss the question of responsibility distribution in networked settings.

20 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 13.

21 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 8.

22 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 14.

23 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 14.

24 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010),14.

25 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 14.

26 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 14, 23 and 25.

27 See also Patrick van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 Computer Law & Security Review 535, 539.

where the factual influence is, and thus based on a factual rather than a formal analysis."[28] In some cases, control over the purposes and means follows directly from a law—for instance when a national law determines that a government body shall process data for a public service such as social security. In other cases, it follows from an implicit competence—when the necessity of data processing follows from another legal relationship, such as an employer having to process employee data. In other cases, the non-legal facts dictate who is a controller—for instance when there is no legal provision or contract in place to determine the data controller, or there is a provision or contract, but the factual situation does not correspond with its stipulations of the contract. This understanding of controller as a "functional"[29] concept as established by the Working Party, remains relevant today, as it is being applied in court cases as well as enforcement action by Data Protection Authorities (DPAs).[30]

2. Joint controller and pluralistic control

20 The Working Party opinions further elaborate the notion of joint control, which in the DPD was captured in the words "*or jointly with others"* in the definition of controller. This limited articulation of joint control suggests that networked data processing was not a focal point of the legislator.[31] But the increasing interconnectedness of digital service offerings, as a result of cloud computing and service integration, increases the importance of a clear conceptual framework for such situations. Without a clear framework to attribute responsibility, it is unclear who is responsible for data protection obligations and to what extent, hampering the effectiveness of data protection law.[32]

21 The main guideline of the Working Party for determining if there is joint (or pluralistic) control is again to apply the functional approach.[33] Thus, joint control is not primarily determined by what the contract between the parties states, but by the factual control they yield over the purposes and means of processing.

22 Furthermore, the Working Party stresses that there can be many different constellations of joint control and it is not necessary that the different parties determine the purposes and means equally.[34] The Working Party does not give clear cut criteria to determine to what extent purposes and means have to be determined together. Instead, it develops a "typology", i.e. a collection of examples, which offer useful guidance but also raise many questions. To illustrate, in the example of behavioural advertising, the Working Party says that if publishers transfer personal information regarding their visitors to the ad network provider, they will be joint controllers.[35] The Working Party later says that when publishers trigger the transmission of personal data like the IP address or cookies—by setting up their website in such a way that the user's browser is redirected to an ad-network provider website— they have "data controller *related* responsibilities".[36] It is unclear how this concept should be interpreted and how it differs from "data controller responsibilities". And do they have responsibility because they are an independent controller, a joint-controller, or even in spite of not being a controller at all?

23 Nonetheless, the following principle can be deduced from the Working Party's opinions. Parties qualify as a joint controller when they determine together the purposes *and* means *to some extent* and *for some part of the data processing*. However, it remains unclear to what extent and to which part of the processing a party needs to be involved in order to be classified as a joint controller.

28 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 1.

29 Which means the concept defines a socio-economic reality, not a formal legal arrangement. In other words, you cannot simply make some organisation a controller or processor by stipulating it in a contract, if the actual control is not in line with the contract.

30 The continued relevance of the concept of "functional analysis" can be seen for example by its use by advocate general Bot in *Wirtschaftsakademie* paras 46, 76 and extended to determining where the location of an establishment of a data controller is located para 92 (See B.III. below). It has been used by DPAs, moreover, in deciding that an organization is a controller even when a contract says that they are a processor (Autoriteit Persoonsgegevens (2018) pp.11-12).

31 Although it was a step in the right direction as the DPD was the first data protection law that had a concept of joint control at all. See Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 17.

32 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 18; See also Christoper Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007), 71-77, indicating that the existence of these unclear situations is not a mere theoretical concern.

33 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 18.

34 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 19.

35 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 18.

36 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 23.

3. Allocating responsibility and liability for joint controllers

24 Allocating responsibility and liability in situations of joint control is one of the central goals the opinion of the Working Party on the concept of controller—"[...] the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules and how data subjects can exercise the rights in practice. In other words: to allocate responsibility."[37]

25 The guiding principle here is that relevant actors are free to distribute responsibilities as long as everything is covered. In cases of joint control, controllers should determine whom among them is responsible (competent, liable) for which of the data subjects' rights.[38] So, for example, in the case of a shared information infrastructure (pool) among banks, the Working Party states that it should be decided who answers data access requests.[39] This may be either the bank of the data subject or the organisation that operates the infrastructure.

26 For the Working Party, a data controller does not necessarily carry complete responsibility for all data protection obligations.[40] They develop two ways of assigning partial responsibility: responsibility for distinct *stages* of data processing; and different *degrees* of responsibility. In situations in which data processing takes place in different stages (or phases), actors may only be responsible for the stages they are part of. For example: " [the] responsibility of a publisher in the context of behavioral targeting, covers the first stage of the processing, i.e. the transfer of the IP address to ad network providers that takes place when individuals visit their web sites [...]."[41] In other words, the Working Party proposes differentiating between processing operations and looking at the question of responsibility more *granularly*. At the same time, it notes that publishers share responsibility for transparency towards data subjects with ad network providers (and they should help to provide information to data subjects) because they are the main interlocutor from the point of view of the data subject.[42]

27 Regarding the degrees of responsibility, the Working Party notes that different actors can be involved in the processing to different degrees, and therefore carry responsibility to different degrees.[43] We interpret this to mean that if multiple actors are involved in the same stage(s) of processing, they nonetheless may not have equal responsibility to uphold specific obligations like the fulfilment of the lawfulness requirement, transparency, or the respect for data subject rights in practice. For example, in opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the Working Party states that SWIFT and financial institutions have a joint responsibility, although to differing degrees.[44] However, it does not offer principles to determine the degrees of responsibility. Later in the same opinion they state that SWIFT must comply with its obligations under the DPD, and member financial institutions in the EU have the legal obligation to make sure that SWIFT fully complies with the law.[45] It seems to us that if financial institutions have to make sure that SWIFT complies with the law, then in the end they have the same degree of responsibility: full responsibility.

28 The Working Party introduces the principle that parties can have partial responsibility, but it does not develop a consistent framework to determine the exact scope and limit of this partial responsibility. While the DPD and GDPR only allow for full responsibility by the controller for all aspects of data protection. This creates a situation where there is no explicit legal basis for partial responsibility, there is no legal framework to distribute such partial responsibility, and there is no coherent guidance of the Working Party. This is an additional source of legal uncertainty.

29 Another issue with the Working Party's analysis is that it presupposes that the different actors are able to work together to make sure that all relevant

37 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 4. Emphasis in the original.

38 For example: Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 22 and 24. "Parties acting jointly have a certain degree of flexibility in distributing and allocating obligations and responsibilities among them, as long as they ensure full compliance".

39 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 23.

40 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 11. "In sum, for these reasons, publishers will have some responsibility as data controllers for these actions".

41 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 18.

42 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 17-19.

43 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 1, 22 and 33; Article 29 Data Protection Working Party, 'Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (2006), 2.

44 Article 29 Data Protection Working Party, 'Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (2006), 2.

45 Article 29 Data Protection Working Party, 'Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (2006), 26.

obligations are met—an assumption that may not hold in practice. It does not identify what minimum responsibilities need to be upheld when cooperation is impossible, or what the consequences of not meeting the minimum responsibilities would be.

30 The last question that the Working Party discusses is how liability for compensating damages (Article 23 PDP and Article 82 GDPR) should be attributed in situations of joint-control.[46] To answer this question the Working Party introduces the concept of "joint and several liability".[47] This means that when a data subject exercises a right, such as the right of access, all joint controllers are liable in relation to the data subject in case of non-compliance—irrespective of how they had determined their obligations among themselves.[48] The controllers can still arrange a certain distribution of the cost of non-compliance, but this arrangement is between themselves and does not affect the data subject. According to the Working Party, "joint and several liability" should only be applied when the distribution of responsibilities as determined by the controllers or by the factual circumstances do not yield an unambiguous conclusion.[49] This opinion does not offer clarity on how to deal with the situation in which this is not the case.

31 As demonstrated by the changes made by the GDPR and the case law discussed further below, the opinions by the Working Party, while not having binding legal character,[50] have impacted the interpretation of the concept of controller and the corresponding allocation of responsibility and liability. But, as we will show, some of the issues identified above also lead to considerable confusion.

III. ECJ decision in Wirtschaftsakademie

32 Given the ambiguities in the law and the Working Party's guidance on the controller concept, it's not a surprise that the ECJ was asked prejudicial questions on several occasions about the determination of data protection responsibility in networked settings. Two of these cases stand out. One is *Google Spain*, decided in 2014, which deals with the responsibility as an independent controller of a search engine.[51] The second case, C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, decided in 2018, deals primarily with determining the requirements for being a joint controller, and the responsibility that follows from being a joint controller.

33 The key facts of *Wirtschaftsakademie* are as follows. A private school, *Wirtschaftsakademie Schleswig-Holstein (WSW),* used Facebook for creating a so-called fan page. When users visited the fan page, a cookie was placed on their computer, but users did not receive a notification about this from Facebook or the school.[52] The Data Protection Authority of Schleswig-Holstein ordered the school to deactivate the fan page because not informing the user of the related processing of personal data breached data protection law.[53] The school contested this decision, arguing that they were not a data controller with regards to this processing.[54] The German courts agreed with the school and ruled in all instances that the school should not be considered a joint data controller.[55] The German Federal Administrative

46 We note that the concepts of responsibility and liability are sometimes used as if they are synonyms, but they are not. Responsibility is much broader concept which includes the questions: "Which actor is legally obliged to make sure all obligations of the law are met?" "Who can be legally held accountable for breaching these obligations?". Being held accountable can be either through enforcement actions by the DPA, or by the courts after an enforcement action initiated by the DPA or a data subject. Liability only refers to the obligation to pay compensation to data subjects in case they have suffered damage as a result of infringements of the law by the data controller. (i.e. Article 82 GDPR and Article 23 DPD). See for a detailed of liability under EU data protection law: Brendan Van Alsenoy, 'Liability under EU Data Protection Law' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271.

47 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 22.

48 The Working Party is not precise enough in its use of the term joint and several liability to unambiguously determine how they interpret it.

49 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 24.

50 Christoper Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007), 10.

51 For a detailed discussion of this case see Eleni Frantziou, 'Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review 761; David Erdos, 'Intermediary Publishers and European Data Protection: Delimiting the Ambit of Responsibility for Third-Party Rights through a Synthetic Interpretation of the EU Acquis' [2018] International Journal of Law and Information Technology 1.

52 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 15.

53 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388,para 16.

54 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 16.

55 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, paras 19, 21 and 23. The German national implementation of the DPD, the Bundesdatenschutzgesetz, did not have any mention of the possibility of joint control. However, from the very early stages of the procedure the DPA refers to the formulation of joint control in the DPD as well as in the Working Party's opinion on the concepts of 'controller' and 'processor'. None of the parties involved questions the existence of joint control as a legal concept;

court asked in preliminary questions to the ECJ if a party who is not a data controller, such as the school in their view, can nonetheless be held responsible for data protection infringements committed by the company they choose to do business with, in this case Facebook, in "multi-tiered information provider relationships".[56]

34 Advocate General Bot (the AG) delivered the opinion for the Court and argues, in line with the position taken by the Working Party, that the decision of who is to be considered a data controller should follow a "functional approach".[57] The AG argues in two ways that the fan page administrator should be considered a data controller. He first argues that the administrator made the choice to use Facebook for creating a fan page and solely by making this choice determined the possibility for Facebook to start data collection. This alone is enough to see them as data controller, according to the AG.[58] The AG's second argument is that a fan page administrator influences the actual processing of data by Facebook, for example by setting filters that determine to whom the fan page will be shown. This *de facto* exercise of influence over the processing constitutes participation in the purposes and means of processing, and therefore leads to the conclusion that the administrator has to be considered a (joint) controller.[59] As a supporting argument for qualifying the administrator as a controller, Bot notes that if the administrator is not a controller, for example because they cannot decide on the further contract between itself and Facebook, then it would be too easy to evade responsibility. Moreover, he argues that by assigning responsibility to less powerful economic actors in their relationship with suppliers, they will start to demand adequate data protection by such suppliers, thus creating positive ripple effects with regards to data protection compliance.[60]

35 With respect to the question of which responsibilities follow from being a joint controller, Bot refers back to the Working Party. He states that shared responsibility does not imply equal responsibility,[61] but does not discuss how this non-equal responsibility should be assigned.

36 In its judgment, the ECJ follows the AG in concluding that the premise underlying the question asked by the German court, i.e. that the administrator is not a data controller, is wrong. The administrator of a fan page, by choosing that particular service, is a data controller, according to the Court. The Court argues that the goal of the DPD is to "ensure a high level of protection of the fundamental rights and freedoms of natural persons".[62] To ensure this aim, the DPD defines the concept of data controller broadly, which in turn helps to ensure "effective and complete protection".[63] In line with these principles, the data controller does not have to be singular.[64] The ECJ adds that the fan page administrator has a role in determining both the purposes and the means of the data processing.[65] One of the purposes of the placement of cookies is to enable the fan page administrator to obtain statistics. By defining the type of statistics, the fan page administrators contribute to the processing. "[T]he administrator of a fan page [...] must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page."[66]

the question is if the concept applies to this case.

56 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 24.

57 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, paras 46 and 76. Interestingly a search of the digital archive of ECJ judgements shows the court itself does not explicitly refer to the term "functional approach" in its analysis of the concept of data controller neither in this case nor in any other.

58 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 56 "Inasmuch as he agrees to the means and purposes of the processing of personal data, as predefined by Facebook, a fan page administrator must be regarded as having participated in the determination of those means and purposes."

59 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 57.

60 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 74.

61 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 75.

62 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 26.

63 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388. The principle of "effective and complete protection" is not only used to argue for a broad definition of controller, but also for arguing for the broad scope of other concepts. In *Google Spain* for example, the same principle is invoked to decide if "processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State". In particular the Court argues that "in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words ["in the context of the activities of an establishment"] cannot be interpreted restrictively. Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* para 53.

64 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 29.

65 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, paras 36-39.

66 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 39.

37 With respect to answering the question regarding which responsibilities follow from being a joint controller, the Court also follows Bot and the Working Party.[67] It adds that "the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case".[68]

38 In the following subsections, we discuss two key elements of the ruling with regards to responsibility in networked settings in more depth: (1) how the concept of controller is interpreted expansively broadening the applicability of data protection law to more actors; (2) how the Court refers to a framework for allocating responsibilities which is insufficiently developed.

1. Extending the concept of controller to guarantee effective and complete protection

39 A ground-breaking aspect of the ruling is that the ECJ settles on a broad interpretation of what it means to determine the purposes and means of processing. The Court goes out of its way to argue that the fan page administrator takes part in determining the purposes and means of the processing of personal data. In doing so, the Court weighs more heavily the need to ensure effective and complete protection, than a more literal interpretation of the law's text would seem to point to.

40 The Court deviates from the conventional doctrine that only actors who determine the reasons and the ends for which data is processed are controllers. For example, in the SWIFT case, SWIFT became a joint controller because it decided, on its own, to share data with US law enforcement. Moreover, according to the *Google Spain* judgment, Google was an independent controller because it processed previously published data for its own independently determined purposes.[69] On the contrary in *Wirtschaftsakademie,* all the lower courts held that the purposes for processing personal data are set by Facebook and by Facebook alone. It is Facebook who designs the whole of Facebook's technical possibilities, and system of ends that it can be used for, such as the ability to compile statistics on users, as well as the means of doing so. The ECJ nonetheless comes to the conclusion that the fan page operator is a joint controller.

41 The crucial step the Court takes to arrive at this conclusion is that, instead of only looking at the general purposes and means of Facebook as a whole, it looks at the individual data processing operations within the system. In particular, it notes that the fan page administrator can request specific statistics to be displayed. If administrators do this, they contribute directly to a specific processing operation conducted by Facebook. Facebook's servers will start processing personal data of data subjects in a way that would not happen without the specific request of the administrator. The Court rules that because the fan page administrator has an effect on the processing, and can even initiate a particular processing operation, that it contributes to determining the purposes and means.

42 This move from what we would call a "macroscopic view" to a "microscopic view" of data processing operations, is a significant expansion of the interpretation of "determines the purposes and means", beyond how it has so far been interpreted. All German courts who had ruled on this case before had come to the opposite conclusion—ruling that the fan page administrator was not a data controller on the grounds that it decided neither the purposes nor the means.[70] And the interpretation by the German courts was argued directly based on the interpretation of determining the purposes and means as it was given by the Working Party.[71]

43 With this far reaching interpretation, the ECJ wants to do justice to the principle that EU law requires the "effective and complete protection" of the right to protection of personal data, while at the same time recognising that responsibility in the data protection legislation is primarily assigned to data controllers. This principle entered the arguments of the ECJ for the first time in the *Google Spain* case. There, it was also used to argue for the need for a wide interpretation of the concept of "data controller"

67 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 43.

68 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 43.

69 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González* [2014] EU:C:2014:317, paras 35-41.

70 *Wirtschaftsakademie Schleswig-Holstein* [2013] Verwaltungsgericht Schleswig VG 8 a 14/12: "Denn vorliegend fehlt es sowohl hinsichtlich der Zwecke als auch der Mittel der Verarbeitung von personenbezogenen Daten der Nutzer der Fanpage der Klägerin an einer von dieser allein oder gemeinsam mit der Beigeladenen bestehenden Entscheidungsgewalt." and Oberverwaltungsgericht Schleswig-Holstein, 04.09.2014 - 4 LB 20/13: "Insbesondere entscheidet sie [the school] nicht gemeinsam über die Zwecke und Mittel der Verarbeitung" and Bundesverwaltungsgericht, case BVerwG 1 C 28.14 [2016] para 27: "Ihre Entscheidung, für ihr Informations- und Kommunikationsangebot auch die Facebook-Infrastruktur zu nutzen, macht die Klägerin nicht zu einer Stelle, die - allein oder gemeinsam mit der Beigeladenen - über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 2 Buchst. d) RL 95/46/EG) bzw. zur verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG".

71 Oberverwaltungsgericht Schleswig-Holstein, 04.09.2014 - 4 LB 20/13, paras 78 and 79.

in light of the purpose of the DPD.[72]

44 An important consequence of the application of this principle is that in many situations one personal data processing system will have a large variety of joint controllers. The potential consequence of applying such a wide interpretation of the wording of the law, to fit the overall principle of data protection law's effectiveness is that while it indeed helps to defend the relevant rights, it also leads to legal uncertainty.[73] That uncertainty would have been less if the Court would have stayed closer to the AG's first argument for seeing the fan page administrator as a controller. Bot argues that when a first actor (i.e. the fan page administrator) makes possible the data processing by another second actor (i.e. Facebook) *and* that first actor accepts the purposes and means of the second actor (even if the actor has no choice but to accept those as is), that actor is participating in determining the purposes and means and should therefore also be considered a data controller.

45 The AG's argument (that an entity is a data controller whenever it makes possible data processing by another actor and accepts the way that the processing is taking place) was not reproduced by the Court. This may be a missed chance for three reasons. First, the AG's interpretation of the concept of data controller is much closer to the text of the law and existing interpretation of the law, since it upholds what we have called a macroscopic view. Second, this interpretation is simpler and easier to handle in practice, more general in formulation and therefore would lead to more certainty about the interpretation of the law. Third, it would be a lower bar to meet, because it does not include the condition that the Court added—that an actor has to contribute to a specific processing operation, for example by setting filters or requesting statistics. It seems to us that this condition is of little relevance, as it seems unreasonable that if Facebook would not offer the so-called Insights function, the fan page administrator would no longer have responsibility for the data processing. An additional consequence of abandoning this condition is that it would lead to the conclusion that more actors are data controllers.[74]

46 In contrast to the extensive deliberation about purposes and means in the opinion of the Working Party, neither the AG nor the Court make any distinction between determining the purposes or determining the means. "Purposes and means" is consistently used as one noun-phrase and there is no discussion if and to what extent both elements are needed to be a controller. Influencing the processing (or agreeing to the processing and making it possible) appears to be enough to qualify as determining both the purposes and the means of that processing operation.[75]

2. Still no reliable framework to assign responsibilities

47 In its judgment, the Court does not offer any clear criteria for determining how responsibilities should be allocated between joint controllers. Within the data protection framework, data controllers are the actors who have the responsibility to ensure compliance with the data protection principles enshrined in the law. The Court rules that an actor is a data controller exactly because it opens up the possibility of assigning data protection responsibility to that actor, thereby contributing to effective and complete protection. But as we have discussed (in section B.II.4) there is no clear mechanism for allocating responsibility in cases of joint control.

48 It is a pity, therefore, that the referring court only asked whether the fan page administrator is accountable for infringements of data protection law predominantly caused by Facebook but did not ask which responsibilities would follow if this is the case. The ECJ does comment that joint control does not always imply equal responsibility: "[given that] operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."[76] However,

72 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González* [2014] EU:C:2014:317, paras 32-34.

73 For a similar argument with respect to the invocation of the need to for effective and complete protection in the *Google Spain* case, see: Eleni Frantziou, 'Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review 761.

74 This would also fit with the Court's auxiliary argument that the responsibility of the fan page administrator is greater because through the fan page, Facebook also processes data of users who do not have a Facebook account. If this argument is central, then it should not matter if the fan page administrator contributes to any specific processing operation. See: Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388 para 41. The Working Party argues in a similar way to Bot, for the responsibility of the publishers, who by allowing for cookies on their websites trigger the processing of data by ad-networks, while visitors only intended to visit the website of the publisher in: Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 11.

75 Both the AG and the Court do mention that the administrator also has its own purpose (i.e. reasons) for using the service, but this is not presented as a necessary condition for being a controller. Moreover, it seems unlikely that there are cases where an actor uses/integrates a service without having a purpose for it.

76 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388 para 43.

the Court does not provide criteria for how these responsibilities should be allocated. Instead, they refer to the arguments made by the AG on this matter, whom in turn bases his argument on the opinion of the Working Party.[77]

49 But as we have shown in section B.II.3, the Working Party is far from clear on this point. The only clear principle for allocation of responsibility in situations of joint control formulated by the Working Party is that the actors – who are joint controllers – should have determined their respective responsibilities amongst each other. We see this principle clearly applied in a declaration by the German DPAs on the responsibilities applied to Facebook fan page operators after *Wirtschaftsakademie*.[78] Even after the decision, the DPAs do not assign any particular responsibility to operators, except for the general obligation to make an arrangement between Facebook and the operators to determine their respective responsibilities for compliance with the obligations.

50 The key legal question, however, is what happens when actors do not actively distribute the responsibilities among themselves—which remains unanswered. The only thing the Working Party has said is that, in such situation, the allocation of responsibilities should follow from the factual circumstances. If we try to apply that principle in this case, it seems reasonable to conclude that Facebook has the necessary control to be able to handle all responsibilities under data protection law, and therefore, using this criterion, Facebook should be responsible.

51 Alternatively, we can consider what the Working Party concluded in its opinion on behavioural advertising: a publisher has a role in providing information to the data subject. This was contingent, however, on the fact that in a situation of behavioural advertising, the data subject interacts with a website which is under the control of the publisher. Since in this case the way that personal data is being processed through the fan page is primarily controlled by Facebook, it would still lead to the conclusion that it is Facebook who should be responsible, as they can implement the appropriate tools and notifications.

52 However, because the Court ruled that the school is a joint controller after which the level of responsibility that each party carries for the various data protection obligations should be assessed, it seems unlikely that the Court intends an interpretation where that level of responsibility is no responsibility at all. This is the main reason the AG argues that by assigning responsibility to less powerful economic actors (in their relationship with suppliers), they will start to demand adequate data protection from their suppliers—thus creating positive ripple effects. While the Court does not repeat this argument, it effectively moves in a similar direction with its principle of effective and complete protection. The intended effect of the increased scope of (joint) data controller in *Wirtschaftsakademie* may be that by making the organisations who use services provided by other parties responsible for making sure that the services they implement live up to data protection standards, the use of non-compliant services becomes a risk. This can create a much needed incentive for actors in networked settings to demand services that do comply with data protection regulation.[79]

53 The Court does not address the fact that there is no existing framework for assigning specific responsibilities to specific "stages" and particular consequences (enforcement actions) to different "degrees of responsibility". Therefore, the reach and limits of the shared responsibility are unknown. Is the responsibility of the fan page operator only restricted to the first "stage" and only to information provision? Or does the operator share responsibility for non-compliance with regards to all data protection obligations? Can the operator be held responsible for non-compliance with regards to a data protection obligation that can clearly only be provided by Facebook, such as providing an option to opt-out of processing, as the DPA that initiated the case asserted?[80]

77 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, paras 75 and 76.

78 Datenschutzkonferenz (DSK), 'Beschluss der DSK zu Facebook Fanpages' (2018).

79 Jonathan R Mayer and John C Mitchell, 'Third-Party Web Tracking: Policy and Technology', *2012 IEEE Symposium on Security and Privacy* (2012), 416-418, note the current lack of market pressure to exercise good privacy practices and the general lack of enforcement of privacy rules, especially in the EU. And similarly, Seda Gürses & Joris van Hoboken note in particular the lack of enforcement on "curators" in Seda Gürses and Joris van Hoboken, 'Privacy after the Agile Turn' in Jules Polonetsky, Omer Tene and Evan Selinger (eds), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2017), 16.

80 See VG Schleswig, 09.10.2013 - 8 A 14/12: The DPA argues that according to the law there should be a possibility to opt out of processing. Facebook does not offer this possibility and the fan page administrator has no way to meet this obligation. Therefore, the only way to halt the non-compliant processing of personal data is by ordering the fan page operator to close the website. "Zur Begründung verwies der Beklagte darauf, dass Nutzungsdaten nach § 15 TMG (u.a. IP-Adresse, die Cookie-ID aus dem Cookie „datr", Familien- und Vorname, Geburtsname) von Nutzern, welche die Fanpage der Klägerin aufrufen, nach § 15 Abs. 3 Satz 1 TMG für Zwecke der Werbung von Facebook erhoben würden, ohne dass die Klägerin als die nach § 12 Abs. 3 TMG i.V.m. § 3 Abs. 7 BDSG für die Datenverarbeitung datenschutzrechtlich verantwortliche Stelle den Nutzer über eine Widerspruchsmöglichkeit unterrichte. Eine technische Möglichkeit zur Beachtung eines Widerspruchs

54 Advocate General Bobek proposes in his opinion in *Facebook-ID* that responsibility should be limited to the stages for which the joint-controllers share purposes and means.[81] The website-operator which integrates a Facebook like button would only have to provide information about, and collect consent for, the stages of collecting and transferring the personal data.[82] While this may respect the principle of limiting responsibility to operations which parties can meaningfully influence, we believe that this interpretation may not respect the Court's principle of effective and complete protection. Imagine a cookie notice that says: "We *collect* your IP address and Browser-ID and *transfer* this personal data to Facebook. We do not know what Facebook does with the data. Click here to accept and proceed." That would not amount to meaningful transparency in practice.

55 One potential alternative source for answering these questions is *Google Spain*, because in that case the Court also had to allocate specific responsibilities to different actors who are involved in processing the same data. In *Google Spain* the Court similarly invoked the principle of effective and complete protection to argue for an expansive interpretation of the data controller concept in the context of search engines and their processing of personal data in search results. But the analogy between the two cases is only partial because the relationship between Facebook and the fan page operator differs in essential ways from the relationship between Google and the publishers whose publications it indexes. The *Google Spain* case revolves around the analysis that Google's processing of personal data "can be distinguished from and is additional to that of the original publisher"[83] and that its "data processing [...] affects the data subject's rights additionally".[84] Because the data processing by Google was additional to that of the original processor, *and* the processing affects the data subject's rights as well, Google must be considered an independent data controller to effectuate that "the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved".[85] Google controlled in every conventional sense the purposes and means of their independent processing. On the contrary, in the *Wirtschaftsakademie* case all data protection obligations could in principle be enforced through Facebook.[86]

56 *Google Spain* nonetheless offers some insight into how partial responsibilities should be assigned. The Court held that the search engine operator has to ensure that processing meets the requirements of the law "within the framework if its responsibilities, powers and capabilities".[87] When we apply this limiting principle "within the framework of their responsibilities, powers and capabilities", developed in a situation of independent control to a situation of joint control, two interpretations are possible: each controller is responsible for what it is able to do—even without proper coordination with other joint controllers. For example, a publisher could inform data subjects about the fact that personal data processing is happening through the use of cookies.[88] Alternatively, it could mean that whenever one of the controllers is able to prevent infringement of data protection laws, they should do so, either by persuading their joint controller to commit to all data protection obligations, or by not integrating the infringing service.

57 In sum, we conclude that the existing frameworks for assigning responsibilities are inconclusive with respect to the question of how far the responsibility of the fan page administrator reaches. The framework developed by the Working Party relies on the active collaboration of joint-controllers to distribute responsibilities but does not specify what to do when this coordination does not take place. The framework derived from *Google Spain* is also unfit to be used in situations of joint control.

bestehe nicht, da Facebook hierfür keine technische Möglichkeit bereitstelle, sodass allein deshalb bereits ein Verstoß gegen § 15 Abs. 3 Satz 1 und 2 TMG vorliege." and "Da die Klägerin keine technische Möglichkeit zur Einrichtung eines Widerspruchsmechanismus habe, gleichwohl aber eine datenschutzrechtliche Verantwortlichkeit bestehe, sei die Anordnung zur Deaktivierung der Fanpage erfolgt".

81 Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*, EU:C:2018:1039, Opinion of AG Bobek, para 101.

82 Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*, EU:C:2018:1039, Opinion of AG Bobek, para 141.

83 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* para 35.

84 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* para 38.

85 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* para 38.

86 Which raises the question why the German DPA did not go after Facebook in the first place. Indeed, the German DPAs may not have the competency to initiate enforcement actions against Facebook, because that competency is given to the DPA in the county where the company has its main establishment (Ireland). An additional reason for the German regulator to go after the fan page instead of Facebook is therefore the issue of jurisdiction.

87 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* paras 38 and 83. This criterion is also referenced by AG Bot in Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 63.

88 Although even providing information cannot be done well without proper information being provided by the other controller. We discuss this in section C.IV.

IV. GDPR

58 The case law discussed above was decided on the basis of the DPD. In this section we discuss the elements that the GDPR adds to the existing system of determining who is responsible for data protection obligations in networked settings and show these additions do not solve the uncertainties we identified above.

59 As mentioned earlier, the definition of data controller remains essentially unchanged. A new provision (Article 26) deals with the allocation of responsibilities between joint controllers. And Article 82 on liability now includes explicit clauses in Article 82(4) and Article 82(5) on liability in situations of joint control.

60 Article 26 on the allocation of responsibilities between joint controllers states the following:

> 1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them, unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.
>
> 2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
>
> 3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

61 Thus, with regards to the distribution of responsibilities, the main rule still is that actors are free to divide the responsibilities among themselves, as long as they make sure that all responsibilities and obligations are met. Article 26(1) adds explicitly that joint controllers should determine their respective responsibilities among each other. Yet, according to Article 26(3), data subjects can still exercise their rights in relation to each of the data controllers, irrespective of the terms of the arrangement between the joint controllers. This can be understood as follows: the agreement that joint controllers make is there to arrange the *practical* division of tasks, while both controllers remain *legally* responsible to enable the data subject to exercise their rights; and they are both liable and risk enforcement action if not.

62 With regards to liability, Article 82(4) lays out that joint controllers "each shall be held liable for the entire damage in order to ensure effective compensation of the data subject," and according to Article 82(5): "Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation *corresponding to their part of responsibility for the damage*, in accordance with the conditions set out in paragraph 2." In effect, this is the same as the joint and several liability which was already proposed by the Working Party.

63 With regards to the provision on fines, in Article 83 GDPR, which is a major addition when compared to the DPD, there are no specific rules to allocate a fine between multiple data controllers in situations of joint control.[89]

64 To conclude, the GDPR does not fill all the gaps in the existing framework for allocating responsibility among joint controllers. As a consequence, national courts will have a hard time to fill this interpretative void and it seems likely that further questions will still have to be settled by the ECJ.

V. Comments and conclusion

65 Despite introducing some provisions that explicitly deal with joint control, the GDPR does not solve the key problems identified before. While there has been a sustained critique within the academic literature on the system of allocating responsibility in the DPD,[90] the key aspects of the framework remain in place. The basic dichotomy between controller and processor remains, and while there is now a more explicit mention of joint control, there is still no system for allocating responsibilities between joint controllers. In particular, when it comes to the concept of "data controller" and the crucial question of what it means to "determine the purposes

89 Article 83(1) GDPR only postulates as a general principle that fines shall be effective, proportionate and dissuasive.

90 See for example Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 Ohio State Law Journal 1217; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179.

and means" of data processing, the formulation remained the same and no extra guidance in the form of recitals or additional articles is given. In light of the developments in the way that personal data is being processed, as well as the clear issues with applying the basic framework to contemporary data processing practices, further adaptation or clarification of the law is called for.

66 The direction taken by the ECJ, in favour of an expansive interpretation of the concept of "data controller" and the possibility of joint control, in order to secure the overall purpose of "effective and complete protection" of the protection of personal data, has become the legal reality. Deciding for what purposes personal data is being processed and on the means of the processing are no longer the only criteria to determine if an actor is a controller. Integrating a service which involves processing data, and having the ability to influence the processing, also leads to the qualification of controller.

67 With regards to division of responsibilities between joint controllers, the GDPR provides some clarification. In networked situations, joint controllers can decide as they like how they distribute the responsibilities among each other internally, as long as all the obligations are covered. With regards to data subject rights, the data subject should still be able to exercise their rights against each controller involved in the processing of their personal data. However, it is still not clear what happens when joint-controllers do not manage this, which is a highly relevant question in practice. The ECJ has pointed to the Working Party's opinion on the concepts of "controller" and "processor" as a source for deciding how responsibility should be distributed between joint controllers. However, we have shown that the framework for assigning responsibilities to different stages of processing and different degrees of responsibilities is underdeveloped; there are no guidelines for assigning specific responsibilities to specific "stages", no clear principles to determine different "degrees of responsibility", nor criteria to connect particular consequences (enforcement actions) to particular levels of responsibility.

68 While one of the key objectives for replacing the DPD with the GDPR was to reduce legal uncertainty,[91] our analysis shows that with regards to responsibility in networked settings, this objective is not met. The key issue it identified regarding legal uncertainty was the "divergences between the national laws implementing the Directive",[92] but the impact assessment that was part of the legislative process underlying the GDPR,[93] also identifies insufficiencies in the responsibility framework: "Although the definitions and concepts of 'controller' and 'processor' remain themselves relevant, they need to be clarified and detailed in specific provisions as regards the obligations, responsibilities and liability of both controllers and processors."[94] Considering this assessment in which the European Commission relied heavily on the Working Party's guidance, it can be considered a missed opportunity that the GDPR does not provide more clarity on the distribution of responsibilities for joint controllers.

69 The extension of the notion of "data controller" by the ECJ may have the most tangible effects in combination with the introduction of fines. The fines have the potential to change the incentive structure under which organizations operate. Article 82 GDPR states in quite general terms that "the imposition of administrative fines [...] shall in each individual case be effective, proportionate and dissuasive". Although there is no explicit system to determine how to deal with situations in which joint data controllers cannot themselves control the conditions which make a certain data processing operation non-compliant, it seems likely that such circumstances have to be taken into account when assessing the imposition of a fine. Nonetheless, the AG (and in less clear terms also the Court) have said that the fact of using an integrated third-party service instead of your internally developed service should not be a way to evade responsibility.[95] Moreover, according to the AG, it neither matters if there is economic power to influence the processing contract.[96] Given the direction that the Court has taken, it is likely that joint controllers can be fined for continuing to make use of services that do not comply with data protection laws. Whether this will cause sufficient pressure on the market for the necessary coordination to take place depends on how Data Protection Authorities and national courts will develop the direction given by the ECJ.

91 COM(2010) 609, "Communication on a comprehensive approach on personal data protection in the European Union adopted on 4 November 2010", 10.

92 COM(2010) 609, "Communication on a comprehensive approach on personal data protection in the European Union adopted on 4 November 2010", 10.

93 SEC(2012)72 final, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"

94 SEC(2012)72 final, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Annex II, 19.

95 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 64.

96 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 61. Following this line of reasoning we would add it should not matter if any compliant alternative is practically available.

C. Practice of data protection in networked settings

70 In this section we will reflect on some of the practical implications of the responsibility framework for organisations and data subjects who operate in a networked environment. We focus on the responsibility to provide information about the data processing to data subjects (Article 13 and 14 GDPR) and on data access requests (Article 15 GDPR). We look at what technical and organisational arrangements organisations need to have in place, to comply with data protection obligations in networked settings. We also look at structures that impede the ability to be compliant. Rather than trying to aim at a full analysis of all the implications of the emerging responsibility framework, we draw from some practical examples in order to gain insight into the challenge of ensuring data protection safeguards are observed by relevant parties.

71 We first discuss how many organisations do not supply an overview of the recipients to whom personal data is disclosed, which seems to indicate that many organisations do not have a good overview of the data flows they are involved in. Having this overview is a precondition for responsible and transparent data processing in networked settings. We then reflect on the system that needs to be in place to avoid this situation by looking at an example of an organisation that records in great detail how data is being shared. Subsequently, we will look at the use of radio-frequency identification cards (RFID cards) in a public transportation system to reflect on the implications on the systems design for data subject rights. Finally, we look at the debate about responsibility for data protection in networked settings between Google and publishers that use their AdSense network.

I. Who is data shared with?

72 When it comes to organising the technical and organisational arrangements needed for data protection in networked settings, having a clear overview of all the inter-organisational streams of personal data is an important first step. Organisations will need this basic information in order to assess for themselves if these exchanges of data with other entities are lawful. Moreover, organizations need to have this information in order to be able to inform data subjects.

73 In a study we conducted in 2017, we found that only 20% of organisations that received an access request informed data subjects about the *specific* recipients of the data.[97] This low rate of specific answers with regards to the recipients of personal data is indicative of a lack of transparency regarding networked situations. The explicit goal of the right of access, according to recital 63 of the GDPR, is that it should allow data subjects to be aware of and verify the lawfulness of the processing. But without information about who accessed the data, an important aspect of the lawfulness of processing in networked settings cannot be assessed.

74 An interesting example drawn from the above-mentioned study is Bol.com, a Dutch online retailer who did disclose with which other service providers they shared data in specific terms. In our case, data was shared with Accountor Nederland BV in order to process payments and with Docdata BV and Fiege BV for shipment. But even Bol.com did not share all the information about the transfer of data to other organisations. One missing category of recipients for instance was social media plugins and other services placing third-party cookies.

75 Most internet users are familiar with notices about cookies when visiting websites. These notifications often indicate that both first as well as third party cookies are used and provide a link to a cookie policy which explains in greater detail the types of cookies used, as well as a list of the third party advertising cookies with links to the privacy policies of those companies. More recently, options are offered to turn third party cookies off. However, in the answer to the access request, none of the organisations provided information about the personal data that had been collected by third-parties through the use of cookies.

76 The Working Party has written that ad network providers should provide access to data subjects,[98] but following *Wirtschaftsakademie,* it is clear that website owners who integrate their cookies and social plug-ins will share that responsibility in many cases. Bot discusses this situation in his opinion in *Wirtschaftsakademie* when he makes a sidestep to another case currently pending for the Court, *Fashion ID*. Like *Wirtschaftsakademie*, *Fashion ID* also deals with a company which makes use of Facebook technology, the so-called Facebook "Like" button.[99] Bot asserts

97 René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review, 10 <https://doi.org/10.14763/2018.3.927> accessed 26 February 2019.

98 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 24.

99 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 67. For a discussion of how Facebook's plug-ins function through the use of cookies see Güneş Acar and others, 'Facebook Tracking Through Social Plug-Ins' (Commission for the protection of

that "Like fan page administrators, operators of websites with embedded social plugins can benefit from the 'Facebook Insights' service and obtain precise statistical information about the users of their website." [100] According to the AG, this leads to the conclusion that a website manager who includes a Facebook like button is also a controller in relation to the data being collected through the Facebook like button.[101] Since the arguments by the AG were followed by the Court, organisations would qualify as a joint controller for the processing of data through the Facebook like button.

77 The question that follows is which responsibilities the website administrator would have as a joint controller? The Court has held that each controller does not have the same responsibility. In the Working Party opinion that the Court refers to in this context, providing information could be best done by the website administrator, while Facebook should answer to access requests. A division of tasks along these lines would be in line with the main principle of Article 26 GDPR that joint controllers should distribute their respective tasks.

78 But what happens if Facebook does not provide access to the data? What happens when either of the actors does not uphold their responsibility?[102] A key aspect of Article 26(3) GDPR is that while joint controllers should distribute the responsibilities, data subjects may exercise their rights of access against each of the controllers. From this, we suggest that a data subject can also direct a request to access to the website administrator, irrespective of the fact that the personal data is collected through the use of cookies by Facebook and the administrator has no access to data. The administrator could solve this practically by redirecting the request to Facebook. However, if Facebook would not adequately comply, the organisation integrating their plugin may also be held accountable. Bobek, the AG in *Fashion ID,* on the contrary argues that that responsibility for data access rights should be restricted to Facebook alone, and also argues that Facebook and the website operator do not have to make an agreement about this.

II. Establishing a traceable data trail

79 Whilst it is hard for data subjects to trace which organisations have received data about them in many cases, it is certainly technically possible to establish a traceable data trail. However, we observe that even when a system is built in this way, there can be other aspects that impede tracing with whom personal data is shared.

80 To ensure transparency about data processing in networked settings, systems would need to be designed to enable this. In our empirical study, Dutch municipalities stood out in the level of detail they provided on the recipients of personal data.[103] The municipalities were able to provide data subjects with a detailed list of all organisations that access their data, including a complete overview of which particular data was accessed by which organisation. The municipalities were able to provide this level of transparency because they all use a central system for processing personal data, and the architecture of this system is designed in such a way that any access to and/or transfer of the data is recorded.[104] The information on specific recipients of personal data in response to an access request is supplemented by a website which contains general information about the organisations that are allowed to access the system.[105] This website also links to the underlying legal documents ("besluiten"). These legal documents under Dutch law create the legal basis for granting access for the organisations to the system and specify the conditions under which organisations can access the personal data. Moreover, the source code for the system is openly available, creating another layer of accountability.[106]

privacy 2017) Version 1.1.

100 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 70.

101 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 72.

102 Clive Norris and Xavier L'Hoiry, 'Exercising Citizen Rights Under Surveillance Regimes in Europe – Meta-Analysis of a Ten Country Study' in Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer International Publishing 2017), 444-446, argue that Facebook does not comply adequately with its obligation to provide access.

103 See René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review, 11 and 20 <https://doi.org/10.14763/2018.3.927> accessed 26 February 2019.

104 The system is called Personal Records Database (In Dutch: Basis Registratie Persoonsgegevens, BRP), the centralised governmental database of personal data in the Netherlands. On an organisational level it can be added that citizens can exercise their right of access through their current municipality of residence. Another interesting feature of the system is that the code is available open source on GitHub. English language information about the system can currently be found at: <https://www.government.nl/topics/personal-data/personal-records-database-brp>.

105 <https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/wie-krijgen-mijn-persoonsgegevens-uit-brp>.

106 See press release by Dutch government (in Dutch): <https://www.rijksoverheid.nl/actueel/nieuws/2017/11/29/broncode-programmatuur-operatie-basisregistratie-personen-openbaar>. For commentary in English: <https://fsfe.org/news/2017/news-20171206-01.en.html>.

81 Even with such a system in place, a clear view of the data trail can be lost. One of the organisations listed in a reply to an access request to a municipality, sent as part of our study, was SNG, the *Foundation establishing a Network of Court Bailiffs*, which had accessed personal data in the database five years prior.[107] SNG is not itself a court bailiff, but rather an intermediary organisation set up to facilitate flows of information from central databases controlled by the municipalities, the Social Insurance Bank and employers, to the individual court bailiffs that seek access to personal data. The problem is that a person would be interested to know who the final recipient of the personal data is, and to find out why a court bailiff accessed the data. Without knowledge of the final recipient, the data subject is unable to verify the lawfulness of the processing. However, SNG was not able to answer which particular court bailiff had accessed the data through their system because they only retained these records for one year.[108] Thus, the link to the final recipient of the data was broken.

82 This form of data sharing through intermediaries, or clearing houses, is very common in networked settings,[109] because coordination of data streams can be more efficiently managed through these specialised actors. But as our example shows, this form of data sharing can also lead to a lack transparency for data subjects. When the first data controller only logs data sharing with the intermediary, and the intermediary does not retain the log of personal data being accessed through its system, data subjects are unable to know who accessed their data and their data rights are diminished. If the right of access should enable data subjects to follow who processes their personal data and verify the lawfulness of the sharing and processing of the personal data, the link should at least be traceable for as long as the last party in the chain processes the data.

83 Does the responsibility framework under European data protection law help to solve the problem? No, because under the GDPR it is still unclear if any actor would be directly accountable for solving this problem. According to SNG's privacy policy they are a data processor and the individual court bailiffs are the data controllers. According to the responsibility framework, this is indeed the case as long as the court bailiffs determine the purposes and means of all the processing by SNG. The answer depends on a functional analysis, stipulating that this depends on which party has the actual control, and that the contract is not determinative. Regardless of the answer to the question of who the controller is, the question is if the GDPR has any provision that directly assigns responsibility in such a way that this situation would not occur.[110]

III. Building privacy preserving intermediaries for shared infrastructures

84 Across many sectors, personal data is governed through centralised specialised organisations. In this subsection we ask how this organisational setup affects the effective use of the right of access. Examples of this can be found in the healthcare sector, where different healthcare providers need to have access to the medical data of patients; public transportation, where multiple public transport companies share a single payment system; and energy sectors, where multiple energy suppliers share the same grid.

85 Organisations that use this model of centralised data processing will have to coordinate how to deal with the obligations regarding data protection, including the right of access. We found that in most cases data subjects are requested to send their access requests to the organisational users of the system. The organisations that run the technical infrastructure are not data subject facing. This form of coordinating responsibility for data access requests is along the lines proposed by the Working Party,[111] as well as the demands of the GDPR.[112]

86 An example can be found in the Dutch public transportation system, which has transitioned to a centralised dedicated Smart-card travel system for its travellers, called OV-chipkaart. This is an RFID based system, similar to systems in use worldwide, that can be used on the national railways as well as on local public transport. In order to build and manage the infrastructure for a centralised digital payment system, the transportation providers set up a new organisation, Trans Link Systems BV. This organisation is owned by the participating public transport providers.

107 More information on SNG (in Dutch) can be found at: <https://www.sng.nl/>.

108 Following a change in the law, SNG now retains records of final recipients for 20 years, thus solving the issue that we found.

109 Examples include specialised data exchanges for personal data processed by the government, in the insurance industry, in the energy sector, but also add exchanges.

110 According to recital 64 of the GDPR, controllers "should not retain personal data for the sole purpose of being able to react to potential requests." The GDPR does not regulate specifically how long information on recipients of the data should be retained. But if we would apply the guiding principle of effective and complete protection, actors should be responsible for making sure there will be no gaps in the data trail.

111 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 23.

112 Article 26 GDPR.

87 One aspect of the technical specification of this system is that very precise movement patterns are being collected at a centralised level.[113] These movement patterns are always connected to an individual card. Because most travellers have a personalised card, which has their name and photo, most movement patterns are directly connected to an individual person.[114]

88 Another aspect of the system, which we found out about by sending access requests to multiple actors in this system, is that the system is built in such a way that not all transport providers have access to personal data. When a traveller has a personalised card from transport provider A, this provider A has access to the movement pattern that the traveller has with that provider, but not to the data related to transactions that traveller has with other transport providers. When that same traveller then uses the same personalised card, which is registered with provider A, to travel with another transport provider B, this provider B cannot access any travel pattern. In relation to provider B, the card functions as an anonymous card. Only the central organisation has access to all travel patterns across all transport providers. But even within the central organisation, access to some information is restricted, so that most employees of the company cannot access the location data.

89 Jacobs has argued that the way OV-Chipkaart is designed is a "privacy disaster" because of its centralised architecture.[115] In particular because a centralised system can easily be used for surveillance, while the non-digital / non-centralised system that it replaced did not have this feature.[116] Regardless of the qualification of such systems, we observe that in order to provide transparency to data subjects, clear information needs to be provided about elements of data protection by design used in such systems, in order for data subjects to understand how their personal data is being processed in these centralised systems.

90 Intermediaries play a decisive role in the data protection features of a system. Article 25 GDPR demands that organisations apply "data protection by design and by default". The main takeaway of this example is that the design of the shared infrastructure has an impact on effectuating data protection in a networked world, and the participating organisations have to critically assess their designs with regards to data subject rights and the joint-controller doctrine.

IV. Coordination between controllers with asymmetric information

91 While the responsibility framework for joint controllers depends crucially on coordination and collaboration between the parties, the reality of the market is that providers of digital services may present "take it or leave it" offers that do not leave any room for genuine coordination. An ongoing dispute between a group of trade associations that represent major news publishers[117] and Google[118] is exemplary of this situation and serves as an example to show the potentially far reaching consequences of the *Wirtschaftsakademie* ruling, as well as the legal unclarity that exists. The dispute started when Google informed publishers, by means of a blogpost, that because of the introduction of the GDPR, the terms and conditions for the use of various services, including advertisement services with respect to data protection, were going to change.[119] The publishers reacted to this with a letter, finding fault with Google's behaviour on three counts.[120] First, the fact that Google identified itself as an independent controller, second that it relied on the publishers for asking for consent for their data processing, and third for allocating liability to them.

113 Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer Netherlands 2010), 289, 293.

114 65% of cards are personalized cards according to Translink jaarverslag 2017 <https://www.translink.nl/TLS_Corporate/media/Beeldbank/Headerfoto's/Cijfers%202017/Jaarverslag-2017-Translink.pdf>.

115 Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer Netherlands 2010), 289, 292.

116 This concern was not merely theoretical. In 2017 Translink was nominated for the Big Brother Award—a prize for the organisation that does most to threaten privacy—for sharing travel data with the Dutch organisation responsible for student loans (DUO) for fraud prevention without a court order.

117 The trade group consists of four major non-profit trade organisations, Digital Content Next <https://digitalcontentnext.org/membership/members/>, European Publishers Council <http://epceurope.eu/about/our-values/>, News Media Alliance and News Media Association. They represent many major digital content companies such as Associated Press, New York Times and Slate, Volkskrant and Reuters.

118 Google is the biggest player in behavioural advertising and accounts for over a third of US digital ad spending <https://www.emarketer.com/content/google-and-facebook-s-digital-dominance-fading-as-rivals-share-grows>.

119 <https://www.blog.google/products/ads/changes-to-our-ad-policies-to-comply-with-the-GDPR/>.

120 Jason Kint, 'Publisher Letter to Google Re GDPR Terms' (30 April 2018), <https://digitalcontentnext.org/wp-content/uploads/2018/04/Publisher-Letter-to-Google-re-GDPR-Terms-042918.pdf> accessed 19 July 2018.

92 The first problem that the publishers indicate is that in the terms offered by Google,[121] both Google and the users of advertisement services are identified as an "independent controller". The publishers claim that in taking this position, Google is claiming rights over data too broadly. Moreover, they believe that Google should offer an option in which Google would operate as a data processor with regards to the data. However, neither Google nor the publishers consider the possibility that they may be considered joint controllers under the GDPR. Given the interpretation of data controller as a functional concept, the terms and conditions agreed upon between Google and publishers would serve as an input, but would not exclusively determine the role an organisation would have for the GDPR.[122] Given the criteria developed by the ECJ in *Wirtschaftsakademie* to determine whether there is a situation of joint control, this may well be the case. AdSense has a reporting function that is in some ways similar to Facebook Insights. With the reporting function, AdSense users can request reports based on categories, such as country.[123] Because the cases are not exactly similar and the criteria developed by the ECJ are not very clear, the determination cannot be made with certainty, but given the prominence of the effective and complete control doctrine, it seems entirely possible that a court would rule that AdSense creates a situation of joint control with respect to some of the data processing going on.

93 The fact alone that Google offers a controller-controller agreement, in which some data protection obligations are delegated to the publisher, signals that Google and the publishers may have to be considered joint controllers. When two controllers are joint controllers they are obliged to determine in an arrangement their respective responsibilities for compliance.[124] Also when the relationship would be one between a controller and a processor, the details of the conditions under which the processor would process data for the controller have to be laid down in a contract.[125] But if two controllers are truly independent controllers, there is no reason to make a contract stipulating who is responsible for which data protection obligations (like obtaining consent). By asking the publishers to ask for consent on their behalf, Google gives - contrary to what the agreement states - another indication that there is a situation of joint control.

94 Which brings us to the second problem raised by the publishers. They argue that they cannot take on the responsibility of asking for consent for Google's processing of data as long as they do not fully know how Google processes data. They argue that: "Placing the full burden of obtaining new consent on the publisher is untenable without providing the publisher with the specific information needed to provide sufficient transparency, or to obtain the requisite specific, granular, and informed consent under the GDPR."[126] This highlights a bigger problem. Many of the data flows that are part of information systems built out of a combination of services are not transparent. The lack of transparency of many of these systems for end-users is well established,[127] but these systems are quite likely similarly opaque to business partners like the publishers. As long as business partners have no transparency regarding the way elements they integrate in their services process personal data, the processing of personal data by these elements cannot be made transparent for the individuals whose data is being processed. For that reason in itself, the use of these elements is in clear tension with the requirement of transparency under the GDPR.

95 The combination of being a joint controller, with the inability to conduct genuine coordination, the intrinsic opacity of the services offered, and the associated potential of non-compliance creates a potential for enforcement actions against companies who integrate third party digital services. The publishers raise the issue that Google's terms indemnify Google for fines that may have to be paid by Google. But as joint controllers, the publishers also run the risk of being fined directly.

121 The 'AdSense Online Terms of Service' can be found at: <https://www.google.com/adsense/new/localized-terms?gsessionid=D0KST4BDIK97GPoA8n_aSIuRkmeQG3gx> and the associated 'Google Ads Controller-Controller Data Protection Terms' can be found at: <https://privacy.google.com/businesses/controllerterms/>. It states:

> "4. Roles and Restrictions on Processing
>
> 4.1 Independent Controllers. Each party:
>
> (a) is an independent controller of Controller Personal Data under the Data Protection Legislation;
>
> (b) will individually determine the purposes and means of its processing of Controller Personal Data; and
>
> (c) will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Controller Personal Data".

122 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 18.

123 See AdSense Help: <https://support.google.com/adsense/answer/160562?hl=en> "For example, to see which devices your ad units were viewed on broken down by country, you would select the Platforms report and then add the Countries dimension".

124 Article 26 GDPR.

125 Article 28(3) GDPR.

126 Jason Kint, 'Publisher Letter to Google Re GDPR Terms' (30 April 2018), 3 <https://digitalcontentnext.org/wp-content/uploads/2018/04/Publisher-Letter-to-Google-re-GDPR-Terms-042918.pdf> accessed 19 July 2018.

127 See for example Jonathan R Mayer and John C Mitchell, 'Third-Party Web Tracking: Policy and Technology', *2012 IEEE Symposium on Security and Privacy* (2012), 413.

96 The opacity of the data processing by Google, as well as the power imbalance that characterises the "take it or leave it" agreement making, is not unique to this case. Many of the building blocks of digital services, such as payment services, user analytics, maps integration and many others, have the same characteristics. For all these situations, *Wirtschaftsakademie* opens the door to enforcement actions against those organisations that integrate the services into their offerings in case of potential violations by the integrated service offerings. But because of the absence of a clear framework of assigning responsibilities, the development of future case law will be necessary to know the scope and limits of the enforcement in such cases.

D. Conclusion

97 In the wake of *Wirtschaftsakademie,* the concept of data controller is wider than it was thought to be before. Users of platforms and organisations who use/integrate services that rely on the processing of personal data are much more likely to be considered a (joint) data controller. However, notwithstanding the specific addition of an article in the GDPR on the attribution of responsibility among joint controllers, it is unclear what the legal consequences are in case the joint controllers do not suitably arrange their responsibility or fail to uphold the terms of the arrangement. These questions will still have to be answered in future court cases. Our discussion of responsibility for access rights shows that coordination of responsibilities is complex in practice, because many organisations do not have a clear overview of data flows, because of power imbalances between different actors, and because data governance is often taking place in separated specialised units. If the principle of "effective and complete protection" that guided the Court in its interpretation of the concept of data controller will also be applied to the application of remedies in case of non-compliance, this will incentivise organisations that integrate or connect to other services to care for data protection aspects of the services they choose.