

CompLex



Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

Andreas G. Meyer

Identifying Controllers and Processors Pursuant to the General Data Protection Regulation

4/2018



UiO **Det juridiske fakultet**

Henvelselser om denne bok kan g j res til:

Senter for rettsinformatikk

Postboks 6706 St. Olavs plass

0130 Oslo

Tlf. 22 85 01 01

<http://www.jus.uio.no/ifp/om/organisasjon/seri/>

ISBN 978-82-72261-68-8

ISSN 0806-1912

Grafisk produksjon: 07 Media AS – 07.no

Abstract:

The rights and freedoms protected under EU data protection law apply to individuals whose personal data are processed. Obligations and liabilities are imposed on the person or entity that processes the individuals' personal data. The extent of such obligations will vary depending on whether the body is considered a *controller* or a *processor*. A controller determines the purposes and means of the processing, while a processor processes personal data on behalf the controller. While this distinction was relatively clear cut when the 1995 Data Protection Directive was applied, organisational differentiation, globalisation and new technologies has made the identification of controllers and processors increasingly complex to assess. Based on the fact that the concepts are taken over to the EU General Data Protection Regulation of 2016, and on my experience during the few months in which I have practiced law, I conclude that the assessment will remain challenging in the future. This thesis seek to provide clarification and guidance as to how one identifies a legal person processing personal data as either a controller or a processor.

Contents

1	Introduction	7
1.1	Background	7
1.2	Research questions and structure	8
1.3	Legal context	9
1.3.1	Methodology	9
1.3.2	Legal sources	10
1.4	Working definitions	11
2	General overview of concepts	13
2.1	Introduction	13
2.2	“Processing” of personal data	13
2.2.1	Scope	13
2.2.2	Defining the processing operation	16
2.3	The “controller”	18
2.3.1	Scope	18
2.3.2	Bodies subject to controller responsibility	19
2.3.3	“Purposes” and “means”	20
2.3.4	The determination of purposes and means	22
2.3.5	Member state law determination of purposes and means of processing	27
2.4	The concept of “joint controllers”	29
2.4.1	Scope	29
2.4.2	Determination of joint control	29
2.5	The “processor”	32
2.5.1	Scope	32
2.5.2	Persons “acting under the authority” of the controller or processor	34
3	Identifying the controller and processor in practice	36
3.1	Introduction	36
3.2	Franchise contractual relationships	36
3.2.1	Concept and roles	36
3.2.2	Marketing operations in franchises	37
3.2.3	Shared platform for customer management	40

3.3	Consultant services	41
3.3.1	Concept and roles	41
3.3.2	Legal consultants	41
3.3.3	Hired consultants	43
3.4	Social networking services	46
3.4.1	Concept and roles	46
3.4.2	User-generated content	46
4	The suitability of the controller/processor distinction	49
4.1	Introduction	49
4.2	Eliminating the processor	51
4.3	Allocating responsibilities to the initiating party	53
5	Concluding remarks	56
5.1	Lex lata	56
5.2	Lex ferenda	57
	Bibliography	58

1 Introduction

1.1 Background

This thesis examines the definition and application of the concepts of “controller” and “processor” under 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 (“GDPR” or “Regulation”).¹ “Controller” is the term utilised to designate the primary subject of obligations under the Regulation. A “processor” is a person or entity processing personal data *on behalf of* the controller, but some obligations under the Regulation apply directly to processors. The concepts were first introduced under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (“DPD” or “Directive”)², and the definition of “controller” and “processor” remain intact under the Regulation. However, processors were only indirectly subject to obligations under the Directive, as opposed to the Regulation.³

In light of the developments in technology and society as such, the concepts are becoming increasingly difficult to apply in practice.

[D]ue to the complexity of the environment in which data controllers and processors operate, and particularly due to a growing tendency towards organisational differentiation in both the private and the public sectors as well as the impact of globalisation and new technologies, these concepts became increasingly complex.⁴

The quotation describes how the European Commission evaluated the concepts of “controller” and “processor” in light of a society much different from the soci-

1 OJ L 119, 4.5.2016, p. 1–88.

2 OJ L 281, 23.11.1995 p. 31–50. The DPD was the first enacted data protection framework by the European Union. For a general overview of the Directive, see Bygrave (2014) p. 53–64.

3 However, some Member States imposed obligations directly on the processor under the Directive. See for instance the Norwegian Data Protection Act of 2000 section 13(1) where the processor must ensure adequate security of personal data.

4 SEC(2012) 72 Final p. 18

ety when the Directive was proposed in 1990. Practice indeed proves that difficulties may arise when applying the concepts.⁵

The GDPR repealed the DPD and was applied in EU Member States as of May 25th 2018. As the Regulation carries over the concepts of “controller” and “processor” from the DPD, the determination of parties subject to the respective responsibilities attached to these concepts is likely to remain elusive.

Even though the definitions remain unchanged, the Regulation impose a change in the application of the concepts. As the GDPR is “binding in its entirety and directly applicable in all Member States”⁶, Member States are obliged to apply the concepts of controller and processor as defined under the GDPR. Variations existed in how the Member States transposed the controller and processor concepts in national legislation pursuant to the DPD.⁷ These variations were eradicated as of the day the GDPR was applied.

This thesis establishes the content of the criteria for identifying a controller and processor respectively. Subsequently, practical scenarios where it is difficult to establish what roles certain parties have under the GDPR are analysed. In conclusion, the thesis discusses the general suitability of the two concepts.

1.2 Research questions and structure

The second chapter of this thesis clarifies the definition of controller and processor under the GDPR, pursuant to Articles 4(7) and (8). The main research question concern the factual circumstances that must be present for the identification of a body as controller or processor. The legal subjects to which such responsibilities may apply are also subject to clarification. To a certain degree, Member States have discretion to regulate controller designation in national legislation, and the thesis will examine the conditions for such nomination. Closely

5 Korff and Brown (2010) p. 28-29. See for instance the Danish Data Protection Authority’s Guidelines on processors and controllers p. 7 and decision PVN-2011-10, where the Norwegian Data Protection Tribunal dissented on whether a law firm was acting as controller or processor. See also C-25/17 *Jehovan todistajat*. An as interesting observation, proving the complexity with respect to controller determination, the Advocate General had to dismiss the fact that preachers in the religious community acting “in response to divine command” could relieve the community from its obligations as a controller.

6 Article 288(2) TFEU.

7 SEC(2012) final p. 16-17. The Irish Data Protection Act of 1998 defined controller as the body who “controls the contents and use of personal data” (section 1), while the German act (*Bundesdatenschutzgesetz*, 2003 section 3(7)) referred to the “person or body which collects, processes or uses personal data for itself, or which commissions others to do the same”.

related to the distinction between processors and controllers is the concept of joint controllers. The thesis also elaborates on the conditions for establishing joint control.

The identification of controllers and processors must always be determined in light of a specific processing operation or set of operations. Against this background, “processing” of personal data is a particularly important concept when allocating responsibilities under the Regulation. In theory and practice, it is therefore important to elaborate on the subject matter of “processing” in this thesis.

Both controllers and processors are subject to various obligations under the GDPR. Their identification is also linked with the liability regime under the Regulation. However, as the *legal definition* of controllers and processors is the subject of this thesis, the legal effects *after* their identification are not examined.

The third chapter applies the established contents of “controller” and “processor” in practice. By identifying the controller and processor in assumed scenarios, the content of, and distinction between controllers and processors are clarified in a practical aspect. The scenarios chosen for the purpose of this thesis relate to situations where it is difficult to assess the respective responsibilities, but also scenarios suitable to analyse the distinction.

In the fourth chapter, the thesis debates the general suitability of the controller/processor distinction by applying a *lex ferenda* perspective. One key question is whether it is necessary to operate with a “processor” under the Regulation, and whether there are any adequate alternatives.

1.3 Legal context

1.3.1 Methodology

To address the research questions, the thesis applies the legal method as laid down by the European Court of Justice. The thesis mainly discusses the descriptive law, *lex lata*, as of the date the GDPR entered into force, but the discussion under chapter 4 relies on a *lex ferenda* perspective.

The CJEU observes the law in the Member States’ interpretation and application of the Treaties⁸, and has jurisdiction to lay down preliminary rulings concerning

⁸ TEU Article 19(1).

their interpretation.⁹ As such, the CJEU establishes the EU legal method. The Court practices an autonomous interpretation of the provision's wording, where the "usual and everyday accepted meaning of that word" makes the starting point.¹⁰ However, the CJEU frequently applies a contextual approach, namely interpreting the provision based on its place "within the scheme of the instrument to which it belongs, and of that instrument in the Community order"¹¹, and based on the purpose of the instrument. An interpretation based on the purpose is generally referred to as a *teleological interpretation*.

Furthermore, the CJEU practices the principle of "effet utile" when interpreting the relevant provisions. In general, the principle implies that "where a provision [...] is open to several interpretations, preference must be given to that interpretation which ensures that the provision retains its effectiveness."¹² Effectiveness in this regard means retaining the provision's "usefulness".¹³

When interpreting the relevant provisions for this thesis, the English language version of the GDPR is the starting point. However, as EU legislation contains several authentic language versions, the thesis will compare these versions where necessary.¹⁴

1.3.2 Legal sources

There is scarce case law where the Court discusses the criteria for determining controller responsibility. Thus, the basis for this thesis' assessments and conclusions is largely the wording of the GDPR, with a teleological interpretation. Some regard is given to the preparatory works in order to illustrate the purpose of the Regulation, but these sources of law do not generally carry great weight in CJEU-practice.¹⁵

As is established in the thesis, there is no indication of any intended changes by the European legislators regarding the concepts of "controller", "processor", and "processing" in the GDPR compared with the DPD. Thus, CJEU practice, preparatory works and legal literature concerning the Directive will also be relevant when establishing the further content of the concepts under the Regulation.

9 TFEU Article 267(1)(a).

10 C-187/07 Endendijk. See also Fredriksen (2012) p. 190-191.

11 See C-327/82 paragraph 11 where the Court expressed that the "interpretation must take into account the context of the provision and the purpose of the relevant Regulations".

12 Joined cases C-402/07 and 432/07 Sturgeon. See also Fredriksen et al. (2012) p. 212.

13 Fredriksen, et al. (2012) p. 212 use the Norwegian term «tjenlig virkning».

14 Ibid p. 192-197.

15 Arnesen, et al. (2004) p. 212-213.

The Court's judgements are preceded by an Advocate General opinion. Relevant opinions are examined in this thesis. Even though the opinion is not legally binding on the Court, it may illustrate and elucidate CJEU practice, and the Court's underlying reasoning.¹⁶ Further, the Court often seems to follow the Advocate General's opinion.¹⁷

The Article 29 Working Party ("WP29"), an independent body set up to advise the Commission¹⁸, has issued an opinion explaining the further content of "controller and processor". The opinion is not legally binding, although WP29 opinions are often referred by the Advocate General and in regulatory processes.¹⁹ Thus, the opinion is discussed in this thesis to illustrate common issues regarding the relevant research questions. The thesis also considers other Working Party opinions where relevant.

1.4 Working definitions

This section explains the concepts used throughout the thesis. The definitions of "controller", "processor" and "processing" of personal data are elaborated in the following chapter.

The definitions of controller and processor are linked with the concept of "personal data". Pursuant to Article 4(1) GDPR "personal data" means "any information relating to an identified or identifiable natural person ('data subject')". For the purpose of this thesis, it is sufficient to note that personal data is a broad notion, which covers any data where an individual is singled out, or where the possibility of such identification is present.²⁰

Data subjects are the identified or identifiable persons to whom the personal data relates, see Article 4(1) GDPR. Data subjects, as natural persons, are the legal subjects who enjoy the rights and freedoms provided for by the Regulation.

16 Fredriksen, et al. (2012) p. 217-218

17 Arnesen, et al. (2004) p. 131. See also Arrebola, et al. (2016) p. 38.

18 Articles 29 and 30 DPD.

19 See for instance the Advocate General's opinion in C-210/16 paragraph 46 and SEC(2012) final p. 14.

20 For a general overview of the concept of «personal data» under the GDPR, see Carey (2018) p. 8-15. Underlining the wide notion of "personal data", the CJEU concluded that "written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute[d] personal data", see C-434/16 Nowak paragraph 62.

When the thesis utilises the term “controller responsibility”, it refers to the fact that an entity is a controller, with all obligations and liabilities imposed on it under the Regulation.²¹

When quoting relevant texts, the thesis sometimes uses italicization to underline important phrases in the quotation. Unless otherwise is specified, the italicization has been added by the author of this thesis.

²¹ For a summary of all obligations imposed on controllers, see Taylor Wessing (2017).

2 General overview of concepts

2.1 Introduction

This chapter primarily discusses the criteria for controller and processor nomination in order to map their distinction. In order to assess the distinction, one must look at the conditions for their designation. Article 4(7) holds that, for the purposes of the GDPR, “controller” means:

...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.

Pursuant to the provision, controller responsibility may be imposed on bodies that “jointly with others” determine the purposes and the means of the processing of personal data. The conditions for imposing joint controller responsibility are also subject to examination in this chapter.

As for the definition of “processor”, Article 4(8) defines it as:

...a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The determination of purposes and means under Article 4(7) is to be assessed in light of “the processing”. As such, the starting point for assigning controller responsibility is to establish whether personal data is being processed. Thus, to provide an adequate examination of the concepts of controllers and processors, this thesis also establishes the content of “processing”.

2.2 “Processing” of personal data

2.2.1 Scope

A fundamental term under the GDPR is the “processing” of personal data, as the scope of the Regulation is explicitly linked to it.²² When an entity or a natural

²² Article 2(1) holds that the GDPR applies to “the *processing* of personal data”.

person processes personal data, that body or individual will be subject to obligations under the Regulation. This presupposes that the derogations under Article 2(2), such as processing “by natural persons in the course of purely personal or household activity”, are *not* applicable. These activities still amount to “processing” but are exempted from the scope of application. However, the Regulation applies to controllers and processors providing the *means* for the processing of personal data for purely personal or household activities.²³

The legislators gave “processing” of personal data a wide area of application under Article 4(2) GDPR:

...‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The legislators wished to apply a technology-neutral concept as the “subject-matter of the rules”²⁴ when introducing “processing” in the DPD. The broad wording provides for a wide scope of protection.²⁵ As stated in Recital 15 GDPR, one object of operating with a wide notion was to “prevent creating a serious risk of circumvention”. The extensive scope is also evident given the exemplification of processing activities, which range from collection, storage and use to the ultimate destruction of the personal data. The wording “such as” must obviously be interpreted as meaning that the list is not exhaustive, signifying that *any* operation performed on personal data is encompassed. Furthermore, it does not matter whether the operations are performed by manually or by automated means – both would make up a processing operation.²⁶

When assessing whether an action constitutes processing of personal data, one must consider whether that action is an “operation or set of operations” performed on the personal data or sets of personal data. Given the wide wording, legal literature in general does not provide a detailed explanation of “operations” in the context of data protection law. However, some useful insight comes from the field of informatics, where data processing is described as “the collection and

²³ Recital 18 GDPR.

²⁴ COM(92) 422 final p. 3.

²⁵ Ibid p. 10.

²⁶ However, manual processing of personal data is only subject to the Regulation with respect to “personal data which form part of a filing system or are intended to form part of a filing system” (see Article 2(1) GDPR).

manipulation of items of data to produce meaningful information”.²⁷ Both “collection” and “manipulation” of personal data would constitute processing under the GDPR. However, as “manipulation” typically refers to alteration²⁸, it could well be argued that the term must be interpreted more widely under the Regulation than in information technology. The provision clearly covers operations that do not constitute collection or alteration; for example, “structuring”, “transmission” and “use”. In addition, nothing in the provision’s wording indicate that the relevant operation has to produce meaningful information in order to constitute processing. Sandtrø argues that there is, nevertheless, a requirement for a “purposive” processing of personal data, as under the GDPR it is required that personal data is collected and processed for “specified, explicit and legitimate purposes” (see Article 5(1)(b)).²⁹ However, under Article 4(2) it is evident that an operation performed *without* any specified purpose amounts to “processing”, but is unlawful pursuant to Article 5.

The CJEU has substantiated the wide definition of processing in various cases. Indeed, the uploading of personal data on an internet page³⁰, transfer of personal data³¹ and communication of minutes of a meeting containing personal data³² all constitute processing of personal data. In C-131/12 Google Spain, the Court held that:

...exploring the internet automatically, constantly and systematically in search of information which is published there, the operator of a search engine ‘collects’ such data which it subsequently ‘retrieves’, ‘records’ and ‘organises’ within the framework of its indexing programmes, ‘stores’ on its servers and, as the case may be, ‘discloses’ and ‘makes available’ to its users in the form of lists of search results.³³

Thus, the operations constituted processing, regardless of the fact that the information had already been published elsewhere. The Court also rejected Google’s argument that the operator carried out the same operations regarding other types of data and did not distinguish between non-personal and personal data.

Given the wide area of application, one may ask whether there are any activities performed on personal data that do *not* constitute processing. The Danish Ministry of Justice implied this in a white paper on the GDPR with respect to the

27 French (1996) p. 2.

28 Oxford Dictionaries (2018).

29 Sandtrø (2016) p. 75-76.

30 C-101/01 Lindqvist paragraph 25.

31 C-201/14 Bara paragraph 29.

32 C-28/08 Bavarian Lager paragraphs 66-69.

33 Paragraph 28.

Danish definition under the DPD. The report, based on practice by the Danish supervisory authority for data protection, states that making available personal data to a processor would not constitute processing of personal data. Furthermore, it suggests that making personal data available to attorneys and accountants for counselling services does not amount to processing.³⁴

It is doubtful whether this interpretation is in accordance with the GDPR. First, the broad wording “any operation [...] performed on personal data [...] such as [...] disclosure by transmission, dissemination or *otherwise making available*” does not indicate exceptions for making personal data available to processors, attorneys and accountants. Second, should the disclosure of personal data to counsellors not be regarded as processing, the operation would not be protected by the rights and obligations under the GDPR. Such an interpretation is arguably not compatible with the overall aim of the Regulation, namely protecting the fundamental rights and freedoms of individuals with respect to protection of personal data.

2.2.2 Defining the processing operation

Article 4(2) refers to “any operation or set of operations” when assessing whether processing of personal data is taking place. The wording does not directly resolve whether multiple operations performed on personal data could be rendered *one* processing operation and, if so, how the actions constituting one processing operation from other operations are determined and distinguished. These questions are of particular interest in this thesis as the controller and processor nomination must be assessed based on the specific processing of personal data.

With regard to the first question, if the legislator did *not* intend to cover multiple processing activities under one processing, it should have omitted “set of operations” from the provision. CJEU practice provides further guidance. For instance, *Tietosuojavaluutus*, where the Court first seems to conclude that the collection of personal data relating to income, the publishing of such data, the transfer of such data to a CD-ROM, and the making available of such data through an SMS-service, constituted one processing operation pursuant to DPD Article 2(b).³⁵ However, in the further assessment, the Court separated the activities when discussing whether the derogations in Article 3(2) DPD apply. In C-342/12, the CJEU labelled the collection, recording, organisation, storage, consultation, use and transmission of personal data “*the processing of personal data*”.³⁶ Thereby, the Court indicated that all activities were to comprise *one* pro-

³⁴ The Danish Ministry of Justice (2017) p. 48-49.

³⁵ C-73/07 *Tietosuojavaluutus* paragraph 37.

³⁶ Paragraph 20.

cessing operation. Further, it would be excessive and impractical to reserve the term “processing” for one single activity. In practice, it would imply that the controller would have to assess the purpose and legal basis for each single activity (for instance, the collection, storing, dissemination and destruction of personal data). Interpreting Article 4(2) in this manner could diminish the effectiveness of the Regulation.³⁷

Concluding that various processing operations may in fact constitute *one* processing of personal data, the question is how one distinguishes processing activities constituting *one* processing from others. The wording of Article 4(2) does not resolve this issue. With respect to the Norwegian Data Protection Act, Schartum and Bygrave argue that a series of operations performed in order to achieve a specified result amounts to the same processing activity.³⁸ In other words, the *purpose* of the processing defines the activities subject to one processing of personal data. As an example, the authors point out that all coherent use of personal data to reach a decision regarding cash benefit is “one and the same” processing of personal data. The same opinion is expressed by Gutwirth, who states that the “delineation and separation of purposes are decisive in the establishment of the number of processing operations”³⁹ and that:

Personal data processing is each processing operation or series of operations with personal data which aims to realise one purpose, one finality. [...] Thus: One purpose equals one processing operation.⁴⁰

The following elements indicate that this viewpoint is valid under the GDPR. The legislative history of the DPD shows that the Commission wanted to use the *processing* of personal data as the subject-matter of the rules, inter alia to allow a general approach to be taken:

...with attention focusing on the data used and the *whole sequence of operations carried out in the light of the objective in view*.⁴¹

The declaration indicates that one sequence of operations is to be viewed in light of its purpose. In this regard, Olsen points out that the definition of controller is linked explicitly to the *purpose* of the processing operation or set of operations.

37 Van Alsenoy (2016) p. 477.

38 Schartum and Bygrave (2003) p. 123.

39 Gutwirth (2002) p. 97.

40 I.c.

41 COM(92) 422 final p. 3.

Thus, strong and legitimate arguments indicate that one may identify the processing operations resulting in a particular outcome as one processing.⁴²

2.3 The “controller”

2.3.1 Scope

The role of controller is imposed on any legal subject that “determines the purposes and means of the processing of personal data” pursuant to Article 4(7) GDPR. The definition resembles the provision under Article 2(b) DPD, which in its time was inspired by the definition of “controller of the file” under the Council of Europe’s Convention 108 (“Conv. 108”).⁴³ The Commission emphasised its desire to “regulate the use of data in the light of the object being pursued” and thus decided to leave out any reference to the words “file” or “data”.

The Convention links controller responsibility to the legal subject who, pursuant to national law, has *legal competence* to “decide what should be the purpose of the automated data file”.⁴⁴ However, the wording under Article 4(7) GDPR provides that controller responsibility must be determined based on factual circumstances. The controller is the body *actually* determining the purposes and the means of the processing, regardless of any competence provided for by law. To illustrate, WP29 holds that the notion of controllers is:

...[a] functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis.⁴⁵

The object is to place the responsibility for ensuring data subjects’ rights on the legal subject exercising control over the processing of personal data. As substantiated by case law, the definition is interpreted broadly to ensure the protection of data subjects.⁴⁶ Although competence in law is not a condition for the imposition of controller responsibility, such competence *may* be provided by the EU member states in their national legislation, pursuant to Article 4(7).

42 Olsen (2015) p. 240-241.

43 Conv. 108 was the first multilateral treaty addressing data protection (see Bygrave (2012) p. 32-41 for an overview of the treaty). COM(2012) 11 final p. 7 holds that the definition of controller was “taken over from” the DPD to the GDPR. COM(92) 422 final p. 10 states, “the definition is borrowed from the definition of the ‘controller of the file’ in the Council of Europe Convention”.

44 Conv. 108 Article 2(d).

45 WP 169 p. 9.

46 C-131/12 paragraph 34.

This section reviewed the elements forming the definition of controller. For the purpose of good structure, the thesis splits the criteria for controller designation into two components: a subjective component where the question is to whom the controller responsibility could apply, and a material component assessing the circumstances determining controller responsibility. The elements in the material component are the interpretation of the “determination” and the “purposes and means”. This section also discussed controller designation where the purpose and means of the processing is determined by EU or member state laws.

2.3.2 Bodies subject to controller responsibility

Pursuant to Article 4(7) GDPR, the controller responsibility may apply to any “natural or legal person, public authority, agency or other body”. This part of the provision was not discussed in the decision-making process when enacting the DPD.⁴⁷ Still, the wording indicates that the scope of controller is far-reaching as both natural and legal persons, including any “other body”, are encompassed. Where processing of personal data by public authorities is subject to the GDPR, such bodies are also subject to the controller responsibility.

Wide as the definition is, the question remains whether it is possible to construct a lower boundary for subjects to controller responsibility. For instance, the Norwegian Data Protection Act, transposing the DPD, assumes that the controller must be entitled to sue and be sued.⁴⁸ Similar limitations are not found in the Danish, UK and French transpositions.⁴⁹ As the definition of a “legal person” may vary between the member states, the important matter is to make sure bodies processing personal data comply with the Regulation, regardless of their formal designation.⁵⁰ Member states must also ensure the data subjects’ right to an effective judicial remedy against controllers and processors not acting in accordance with the Regulation (see Article 79 GDPR).

The responsibility as a controller is not reserved for legal entities but may also apply to natural persons should they determine the purposes and means of the processing of personal data. As an example, the CJEU imposed controller responsibility on a natural person in case C-101/01 Lindqvist. However, an entity processing personal data cannot *appoint* a natural person to be a controller, so long as the determination of purposes and means lies with the entity. Nor is controller responsibility imposed on natural persons with decision-making

47 WP 169 p. 15.

48 Ot.prp. nr. 92 p. 103. Sandtrø (2017) p. 91.

49 See the Danish Data Protection Act section 3(4). For the UK, see Data Protection Act 1998 section 1. For France, see Federal Data Protection Act section 3(7).

50 WP 169 p. 15 seems to share this viewpoint.

power within a company (for instance the members of a board), but rather the company as an entity.⁵¹

Supporting this view, the Advocate General indicated a reluctance to impose the sole controller responsibility on religious preachers, as natural persons, rather than on the religious community.⁵² WP29 holds that “preference should be given to consider as controller the company or body as such rather than a specific person within the company”.⁵³ Board members of an entity, or individuals working for that entity, would be persons acting under the authority of the controller.⁵⁴

Still, where a natural person determines the purposes and means of processing activities, he or she is clearly a controller and subject to all obligations and liabilities imposed on controllers under the GDPR. This was the case in a judgement by the British High Court of Justice, where a senior IT auditor had leaked personal data on his co-workers because he held a grudge towards his employer, Morrisons. Thus, the employees who had their personal data disclosed claimed compensation from Morrisons. When allocating responsibilities, the High Court held that:

What, to the contrary, is consistent with the greater security and protection of the data subject is to impose the obligations of data controller upon such an employee [...] whilst retaining his employer’s vicarious liability for his wrongdoings.⁵⁵

As such, the employee was the data controller with respect to his unlawful processing, but Morrisons remained vicariously liable for his actions.

2.3.3 “Purposes” and “means”

It is the “purposes” and “means” of the processing of personal data that is subject to the controller’s determination. Pursuant to the provision, *both* elements must be determined in order to deem an entity the controller. This section establishes the content of those components.

With regard to the “purpose” of the processing, the Regulation refers to the overall object of the processing, which, as discussed above, is a particularly important element in data protection law. As WP29 points out, the body determining the purpose of the processing is the body that determines *why* the pro-

51 Voigt and von dem Bussche (2017) p. 18.

52 C-25/17 paragraphs 66-73.

53 WP 169 p. 15.

54 This concept is examined in section 2.4.1.

55 *Various Claimants and Wm Morrisons Supermarket PLC* paragraph 154.

cessing is taking place. The link between controller designation and the determination of purpose was enacted in the DPD as the Commission sought to place responsibility for data processing on the body “ultimately responsible for the choices governing design and operation of the processing carried out”.⁵⁶ The declaration indicates that the body responsible for such choices would normally be the body determining the purpose of the processing.

With respect to the “means” of the processing, the provision indicate that the body determining the way in which the purpose is achieved is the data controller, namely, as WP29 states, the body that determines the *how* of the processing. “Means” is a comprehensive notion and could possibly refer to the physical machinery governing the processing and to the formal organisation of the processing.⁵⁷ The French language version refers to “moyens”, reflecting *means* or *methods*, while the German version refers to “Mittel”, indicating *tools*, *instruments* or *methods*.

In its interpretation of “means”, WP29 distinguishes between technical and organizational means and *essential elements*. It is argued that the essential elements are what the legislators intended to cover by means. These “means” take into account the personal data to be processed, how long it will be processed for, and the bodies that will have access to it, namely the *what*, *when* and *who* of the processing. According to the WP29 opinion, technical and organisational means could be delegated to a data processor while the essential elements are “traditionally and inherently reserved to the determination of the controller”.⁵⁸

The preparatory works support this point of view. In the amended proposal for the DPD, the controller would be the body determining “which personal data are to be processed, which operations are to be performed upon them, and which third parties are to have access to them”⁵⁹, thereby indicating the core content of “means” in the consolidated Directive. To underline this point, the Regulation impose certain obligations directly on the processor. For instance, Article 32(1), under which the processor must implement “appropriate technical and organisational measures”, inter alia taking the nature of the processing into account. It would be meaningless to impose such a requirement on the processor, if it was not intended to allow for a certain margin of manoeuvre concerning the technical and organisational means of the processing.

56 Com(92) 422 final p. 10.

57 Büllesbach et al. (2010) p. 38.

58 WP 169 p. 14.

59 Com(92) 422 final p. 10. WP 169 p. 14 also substantiates the distinction based on the preparatory works.

However, the overall purpose of linking controller designation to the determination of purposes and means of the processing was to allocate responsibility to the body able to influence it. Against this background, it cannot be ruled out that too much autonomy for a processor in determining organisational and technical measures with respect to the processing may indeed result in the processor having to assume controller responsibility. This is illustrated by the SWIFT case, where a Belgian global financial messaging service was found to have breached the data protection principles under the DPD because they transferred personal data to US authorities for the purposes of terror investigations. SWIFT gave no notification of the transfer to data protection authorities, its financial institutions, or data subjects.⁶⁰ The Belgian data protection authority investigated and concluded that SWIFT was a controller for that processing, although the proceedings were eventually closed.⁶¹ However, WP29 went further, and concluded that:

...the hidden, systematic, massive and long-term transfer of personal data by SWIFT to the UST in a confidential, non-transparent and systematic manner for years [...] constitutes a violation of fundamental European principles.⁶²

SWIFT claimed to be merely processors for the financial institutions, but WP29 held that SWIFT was a controller in its own right, regardless of the service contract with the financial institutions. WP29 found that SWIFT decided “autonomously on the level of information [...] provided to the financial institutions in relation to the processing”⁶³ and that the management had “the power to take critical decisions with respect to the processing, such as the security standard and the location of its operating centres”.⁶⁴ The financial institutions had no authority regarding the means of the processing other than cancelling the service agreement.

2.3.4 The determination of purposes and means

Pursuant to Article 4(7), the controller is the body *determining* the purposes and means of the processing of personal data. “Determines” is closely linked with the “purposes” and “means”, but each element of the assessment could be regarded separately. Reading the provision, the identification of the controller correlates with the authority to issue instructions and not the actual performance of data processing. Thus, a controller does not have to perform any processing operations itself, but rather exercises determining influence over it.

60 See WP 128.

61 Hogan Lovells (2009).

62 WP 128 p. 26.

63 Ibid p. 17.

64 I.c.

When establishing whether a person or an entity “determines” the purposes and means of the processing of personal data, the provision clearly indicates that decision-making power is emphasised.⁶⁵ This view is supported by the amended proposal for the DPD, where the Commission declared that the responsibility should apply to “the person *ultimately responsible for the choices* governing the design and operation of the processing carried out”.⁶⁶

In C-131/12 (see section 2.2.1), one key issue was whether an operator of a search engine, Google Inc., was the controller in respect of the processing of personal data carried out by its search engine under Article 2(d) DPD. The Court answered in the affirmative and maintained the activity of the search engine played a “*decisive role* in the overall dissemination”⁶⁷ of the personal data in question. It was further held that the organisation of information published online and making it available to users in a structured way, made the activity of the search engine “*liable to affect significantly*” the fundamental rights to privacy and data protection. The Court also stated that it would be contrary to the objective of the provision, ensuring “effective and complete protection of data subjects”, to exclude the operator of a search engine from controller responsibility. Thus, the Court amplified two important points: first, a decisive role in influencing the actual processing; and second, the capacity to influence the data subjects’ rights indicate controller responsibility.

In addition, van Alsenoy argues that the decision indicates that a controller is not required to be “aware of the fact that he or she is processing personal data”⁶⁸, meaning controller responsibility may be imposed regardless of any active decision to process personal data that a body “knows to be personal in nature”.⁶⁹ This interpretation establishes the question of whether an entity may be deemed to be a controller if it does not wish to process personal data.

In the Google Spain case, Google clearly determined the purposes and the means of the processing activities performed through the search engine. As such, it could not escape controller liability by arguing it had no knowledge of the types of information served through third party websites.⁷⁰ Distinguished from this particular case are situations where a body does not wish to concern itself with the processing of personal data. For example, if a data subject transfers personal data to a body without the latter having any wish or intent to pro-

65 Voigt and von dem Bussche (2017) p. 19.

66 COM(92) 422 final p. 10.

67 C-131/12. The relevant extracts from the judgement are found in paragraphs 32–41.

68 Van Alsenoy (2016) p. 478.

69 I.c.

70 Wolf (2014) p. 549.

cess it, that body would not be a controller as it does not determine the purposes and means of the processing. However, should the body decide to use the personal data for its own purposes, it would be the controller with respect to those processing operations.

In case C-210/16, the CJEU concluded that an administrator of a Facebook fan page was a joint controller⁷¹ with Facebook with respect to the processing of the personal data of individuals visiting the fan page. The Court first asked whether the administrator “contributed, in the context of [the] fan page to determining, jointly with [Facebook], the purposes and means of processing the personal data of the visitors to the fan page”.⁷² The Court did not provide an extensive interpretation of the term “joint controller”, but rather based its assessment on the administrator’s influence over the processing.

It was emphasised that, by using Facebook’s services, a fan page administrator subscribed to the fact that the visitors’ personal data would be processed in order to produce viewing statistics. The processing would not have occurred without the decision to create and operate the fan page. Further, the fact that the administrator could influence the specific way in which the tool for compiling viewing statistics was used indicated controller responsibility. By using parameters, the administrator could modify the audience for his page (for instance, defining a personalised audience for marketing purposes). By using Facebook’s tools, the administrator could select categories of individuals whose data would be collected by Facebook and choose what personal data would be collected (for instance, demographic and geographical data). On these grounds, the Court considered the administrator to take part in the determination of the purposes and means of the processing of personal data of visitors on the page.

The Court also discussed whether the fact that the administrator received the personal data in anonymised form could relieve it from its responsibilities as a joint controller. The Court rejected the argument by referring to the fact that the anonymised data was based on the prior collection of personal data by using cookies. Further, having access to personal data was not a condition for imposing joint controller responsibility.

The fact that the administrator used a platform provided by Facebook could not free the administrator from responsibilities as a controller. This is in line with the Advocate General’s opinion. Had the administrator created its own website

71 The notion of “joint controllers” is further assessed in section 2.4.

72 C-210/16 paragraph 31. The relevant extracts from the judgement are found in paragraphs 25–44.

and processed data in the same manner, it would clearly be a controller with respect to that processing. An information provider was not “meant to be able to absolve itself, by choosing a particular infrastructure provider, of the legal data protection obligations toward the users of its information offering that it would have had to meet if it had acted as a mere content provider”.⁷³ Thus, the fact that one party unilaterally determines the contractual terms cannot relieve the other party from controller responsibility.⁷⁴ As a final point, the Court stated that recognising fan page administrators as controllers would ensure greater protection of the rights of those visiting the page, applying a teleological interpretation.

In case C-25/17, the question was whether a religious community was a joint controller together with its members who performed door-to-door preaching activities. The religious community argued that the preachers collected the personal data individually without any disclosure to the community, meaning the collection was “entirely beyond [their] control”⁷⁵. The Court nonetheless concluded that the religious community was a joint controller and based the conclusion on the following facts.

The determination of purposes and means did not have to be carried out “by the use of written guidelines or instructions from the controller”. This line of reasoning should be read in light of the Advocate General’s opinion, who pointed out that “excessive formalism would make it easy to circumvent the provisions” and that the analysis should be based on a factual rather than formal analysis.⁷⁶

The key point in the assessment was, as the Court stated, whether the community “exerts influence over the processing of personal data, for [its] own purposes”, and if the community “participates, as a result, in the determination of the purposes and means of that processing”.

By arranging the preaching activities, allocating areas of activity among the preachers and monitoring it and keeping records of individuals who did not wish visitation, the community “encourages its members who engage in preaching to carry out data processing in the context of their preaching activity”. The organisation and coordination of preaching activities by its members, helped achieve the objective of the community, which was to spread its faith. Thus, members engaged in the preaching, did so for the purposes of the community.

73 The Advocate General’s opinion in C-210/16, paragraph 65.

74 For instance, an employer uploading employee personal data onto a cloud service is still a controller, even if the contract clauses with the cloud provider are non-negotiable.

75 C-25/17. The relevant extracts from the opinion are found in paragraphs 63–75.

76 The Advocate General’s opinion in C-25/17. The relevant extracts from the opinion are found in paragraphs 60–73.

These arguments led the Court to conclude that the community influenced the determination of the purposes and means.

The Court further rejected the community's argument that controller responsibility could not be imposed because the community did not have access to the personal data collected by its members. This is in line with the Court's reasoning in C-210/16.

In its opinion, WP29 stresses that controller responsibility must be determined based on factual influence. The holder of such influence could be indicated in a contract between two parties, but what the contract states is not decisive. Other elements in the assessment are "the degree of actual control exercised by a party, the image given to data subjects and reasonable expectations of data subjects on the basis of this visibility"⁷⁷.

As emphasised in the abovementioned case law, actual control and influence is clearly an essential element in the assessment. A party exercising control over personal data processing is normally the party with the possibility of influencing it. Influence could, for instance, be the ability to bring the specific processing to an end, and the ability to influence how the personal data is processed.

As for the image given to data subjects and their reasonable expectations, these aspects of the assessment cannot be fetched directly from the wording of Article 4(7). One may even argue that imposing controller responsibility based on the data subject's subjective comprehension is contrary to the *de facto* assessment that should be made according to WP29 and the cases referred to above. Nonetheless, it was pointed out by the CJEU in *Google Spain* that "controller" had to be interpreted in a wide sense, and that the capacity to influence the rights of the data subject could indicate controller responsibility.

Still, identifying the controller based on the "image given to data subjects" may not always reflect the responsibilities to the body that in fact has any influence with respect to complying with the obligations and enforcing data subjects' rights under the GDPR. The outsourcing of HR-related processing activities to a third party should not necessarily deem the third party a controller, even though employees communicate with them regarding services and enquiries. Further, emphasizing the data subjects' viewpoint as an element in the controller assessment could cause unpredictability for the entities involved in the data processing. One object of the GDPR is, after all, to "provide legal certainty and trans-

⁷⁷ WP 169 p. 11-12.

parency for economic operators” (see Recital 13). Legal certainty is a fundamental principle in European Union Law.⁷⁸

If in doubt when attempting to identify the controller, one should look at the overall purpose of operating with a controller in the Regulation. Although not expressed directly in the Regulation or the legislative history, it is evident that the purpose of operating with a data controller is to ensure the fundamental rights and freedoms of natural persons with respect to the protection of personal data, pursuant to Article 1(2) GDPR. Another object is to prevent the outsourcing of processing activities reducing the protection of data subjects.⁷⁹ The obligations of processing in compliance with the data protection principles are imposed on the controller⁸⁰, and the controller is subject to the obligation to provide information, ensure data subject access, and other enforcement of data subjects’ rights.⁸¹ To allow data subjects to exercise those rights effectively, the GDPR must provide a “clear allocation of responsibilities”.⁸²

Thus, rather than applying visibility towards data subjects as an element in the controller assessment, the determination of controller responsibility should be based on the objects as referred above, in line with EU legal method. Essentially, one should ask which party is *actually* in a position to enforce the rights of the data subjects and which party may *in fact* influence the processing of personal data so that it is in compliance with the obligations imposed under the GDPR. When discussing whether an assumed processor is in fact a controller, one should ask whether its influence over the processing renders it necessary to impose controller responsibilities to ensure adequate protection of data subjects. These elements of the assessment have support in the wording of Article 4(7), the object of the provision in light of the Regulation as a whole, as well as the cases referred to above.

2.3.5 Member state law determination of purposes and means of processing

The second sentence under Article 4(7) GDPR stipulates that:

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.

78 Craig and de Búrca (2015) p. 558-564.

79 COM(92) 442 final p. 34.

80 See Article 5(2) GDPR.

81 Articles 12–20 GDPR. See Recital 25 DPD, which states that the principles of data protection must be reflected in the obligations imposed on controllers, and in the rights conferred on individuals, such as the right to information.

82 Recital 79 GDPR.

The provision governs instances where Union or national legislation determines the purposes and means of processing of personal data. This is often the case, and one legal basis for processing of personal data is where it is “necessary to comply with a legal obligation to which the controller is subject”.⁸³ Thus, it is clear that controller responsibility may be imposed on bodies not determining the purposes and means of the processing.

At the same time, the provision limits the margin of manoeuvre for member states when it comes to imposing controller responsibility. The wording of the provision clearly indicates that member states may *only* impose controller responsibility or the criteria for its nomination in their legislation where the purposes and means of the processing are *in fact* determined by Union or member state law. As the controller should be a body with influence over processing, interpreting the provision in this manner would also best ensure the freedom and protection of natural persons.

When considering whether “Member State law” determines the purposes and means of the processing, one must first assess the requirements for legislation to be qualified as “law”. Recital 41 GDPR provides guidance in this regard, stating that:

Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it.

Against this background, the Regulation does not impose any formal requirements, meaning administrative regulations, secondary law, customary law, and even decisions by public bodies, may qualify as “law”. However, such rules must be foreseeable to natural and legal persons subject to them and fulfil the requirements of clarity and preciseness. In “foreseeable”, one must interpret a requirement for the rules to be publicly available, as bodies need access to the rules to predict their legal position.

Member state law may explicitly appoint a body as a controller, or more indirectly impose on it a task that, by its nature, requires processing of personal data.⁸⁴ As an example of explicit appointment, see the Norwegian National Insurance Act. Under section 21–11a fourth paragraph, the Norwegian Directo-

⁸³ Article 6(1)(c) GDPR.

⁸⁴ WP 169 p. 10.

rate of Health is explicitly appointed controller for the processing of personal data for the purpose of benefit distribution. However, the latter scenario is more common. In this regard, the Norwegian Working Environment Act section 5-1 first paragraph requires the employer to keep records of all personal injuries occurring during the performance of work. As, by its nature, the duty requires processing of personal data, the employer is the controller for that processing.

2.4 The concept of “joint controllers”

2.4.1 Scope

The definition of “controller” under Article 4(7) GDPR holds that controller responsibility may be imposed on a body that “alone or jointly with others” determines the purposes and means of the processing of personal data. The existence of “joint controllers” is also evident pursuant to Article 26 under which obligations are imposed on “two or more controllers [who] jointly determine the purposes and means of processing”.

As such, two or more bodies may share controller responsibility should they together determine the purposes and means of the processing of personal data. Article 26 GDPR imposes duties on joint controllers to determine their respective responsibilities for compliance with the Regulation through an “arrangement”. This is not to be understood to mean joint controllership cannot exist without such an arrangement. WP29 holds that “the assessment of joint control should mirror the assessment of ‘single control’”⁸⁵, thus indicating that the elements of control, influence and possibility to enforce the rights of data subjects as discussed under section 2.3.2 is determinative. Against this background, two entities may be joint controllers without any arrangement between them. However, this would constitute a breach of Article 26.

Practice proves that it may be difficult to establish whether there is joint determination of purposes and means. An important question is to what extent control must be exercised jointly.

2.4.2 Determination of joint control

The wording under Article 4(7) does not provide any guidance regarding to what extent two parties must determine purposes and means jointly. However, in legal theory it is assumed that joint control does not need to be corresponding. As WP29 maintains, “joint determination may take different forms and does not need to be equally shared”. This viewpoint is underlined by the Advo-

85 WP 169 p. 18.

cate General's opinion in C-210/16, which emphasised that it is not necessary to have "complete control over all aspects of data processing"⁸⁶ to be regarded as a controller. Interpreting the provision in this manner is reasonable in light of its object. First, it would be impractical with a requirement of equal control as it would make it difficult to allocate responsibilities in practice. Second, factual influence should be a determining factor when assessing responsibilities under the GDPR. Such influence may be significant, even though the determination of purposes and means is not equal between two parties.

In C-210/16, the court held that "the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing."⁸⁷ This statement is more difficult to reconcile with the wording under the GDPR. Pursuant to Article 26(3), a data subject may exercise his or her rights "in respect of and against each of the [joint] controllers". Further, Article 82(2) holds that "*any* controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation". It is thus clear that each of the joint controllers are *principally* liable for compliance with the GDPR, at least towards the data subjects. The fact that joint controllers may allocate responsibilities internally does not mean their respective responsibilities are not "equal" pursuant to the Regulation.

As when identifying the controller, joint controllers must be determined in light of a specific processing operation or set of operations. Pursuant to the enactment of the DPD, the concept of two or more controllers was amended by the Parliament, and the Commission found that it provided "for the possibility that *for a single processing operation* a number of parties may jointly determine the purpose and means of the processing to be carried out."⁸⁸ In this context, WP29 holds that the processing operations must be examined at both micro and macro level. Although certain processing operations may appear disconnected at micro-level as they have different purposes, one should "double check whether at macro-level these processing operations should not be considered as a 'set of operations' pursuing a joint purpose or using jointly defined means".⁸⁹

Olsen and Mahler utilise a four-category form when assessing joint control.

⁸⁶ Advocate General's opinion in C-210/16, paragraph 62.

⁸⁷ Paragraph 43.

⁸⁸ COM(95) 375 final-COD287 p. 3.

⁸⁹ WP 169 p. 20.

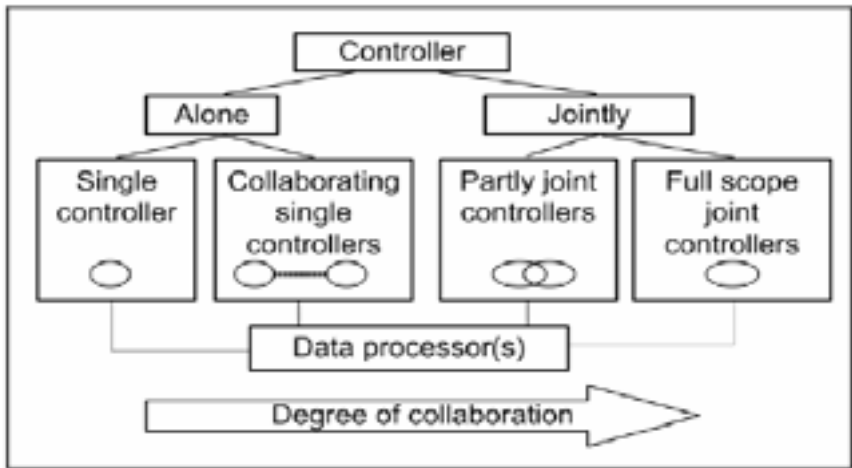


Figure 1: Four-category form for assessing joint control. Illustration from Olsen and Mahler (2007) p. 22.

To be regarded “joint” controllers, two or more bodies must either determine purposes and means of some processing operations in light of a larger chain of operations, or jointly determine all purposes and means of the chain of operations.⁹⁰ Joint controllership is only applicable for those processing operations where the purposes and means are determined jointly, namely the area covered by both circles in the illustration. Two bodies that collaborate with respect to the processing but determine purposes and means independently would be collaborating single controllers rather than joint controllers.

The wording of Article 4(7) clearly indicates that both the purposes *and* the means of the processing must be determined jointly. One may thus ask whether it is within the scope of “joint controllers” if two bodies only determine *one* of those elements jointly for a specific processing activity. WP29 argues that “sharing only purposes or means” may still amount to joint control.⁹¹ Notwithstanding the fact that *sharing* purposes or means are *not* the criteria for assessing controller responsibility as this is the *determination* of those elements, the statement seems justifiable with respect to the clear allocation of responsibilities. Where a party has great influence in determining essential means of the processing, inter alia by determining who shall have access to the personal data in

⁹⁰ Ibid p. 22-23.

⁹¹ WP 169 p. 19.

question, it may still be deemed a joint controller even if it does not determine the purposes of that processing. De facto, the party would be liable to affect the processing of personal data, and thus influence the rights and freedoms of the data subjects.

In case C-25/17, the Court held that access to personal data is not a condition for imposing joint controller responsibility. Underlining this, the Advocate General held that the “inability to fulfil directly all the obligations of a controller, such as right of access, does not exclude the possibility of being a controller”.⁹² This finding is in line with the object of the GDPR. A body may well determine means and purposes of processing and thus influence it, even if it does not have access to the personal data.

2.5 The “processor”

2.5.1 Scope

Pursuant to Article 4(8) GDPR, the processor is “the natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller”. The qualifying criterion when determining whether a party is a processor is essentially whether the processing is carried out *on behalf of* the controller. The wording “on behalf of” seemingly refers to actions taken in the interest of another party, meaning the processor processes personal data in the interest of the controller. Thus, the processor does not itself determine the purposes and the means of the processing, but processes personal data to fulfil the controller’s defined purposes. Its existence depends on “a decision taken by the controller, who can either process data within its organisation [...] or delegate all or part of the processing activities to an external organisation”.⁹³ One may thus conclude that two elements must be in place in order to identify a body as a processor: the processor must process personal data on instruction from the controller, and must perform the processing in such a way as to achieve the controller’s defined purpose(s).

It is the *processing of personal data* that is to be carried out on behalf of the controller. Service providers offering services where personal data processing is necessary are not always considered processors. For instance, a forwarding agent need the name and address of the recipient in order to ship a parcel. When the sender provides that information to the agent, the agent is a controller in its own right with respect to such data. The agent determines the purposes for the

⁹² The Advocate General’s opinion in C-25/17 paragraph 71.

⁹³ Voigt and von dem Bussche (2017) p. 20.

processing, providing a delivery service, and also the means, how such data is processed and the personal data required to provide the service.

As when identifying the controller, the identification of the processor must be assessed in light of a specific processing operation or a set of operations. Pursuant to the wording under Article 4(8), a body may *only* be considered a processor in the context of processing carried through on behalf of the controller. The controller will normally define a purpose for these processing activities, which should thus be considered as one processing.⁹⁴ Where the alleged processor determines its own purposes, even for the exact same processing activities, we are dealing with a *different* processing of personal data. This processing is *not* carried through on behalf of the controller, and since the alleged processor determines the purposes and means in this regard, it would be the controller in the context of that processing. This is codified under Article 28(10) GDPR, which holds that:

Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

The provision indicates that the processor is considered a controller for the processing of personal data for which it determines the purposes and means. In the proposal for the GDPR, the provision read that under these circumstances the processor would “be subject to the rules on joint controllers”.⁹⁵ The text was adopted by the Parliament⁹⁶, but amended in the Council’s position.⁹⁷ As the final text does not include any reference to “joint controllers”, the indication is that the rules on joint controllers are not automatically applicable in situations to which the provision refers. This interpretation is also in line with the wording and purpose of the provision. First, where a processor processes personal data on its own behalf, outside the scope of the controller’s instructions, there would not be any “joint” determination of means and purposes. Second, automatic applicability of the rules on joint controllers would allow the “controller-turned-processor” to put undue pressure on the controllers, as the processor’s unscrupulous processing would affect the liability of the controller.⁹⁸

94 See section 2.2.2.

95 COM(2012) 11 final p. 58.

96 P7_TC1-COD (2012) 0011 p. 168.

97 Doc. 5419/16 p. 157.

98 Treacy (2012) p. 4.

In its opinion, WP29 maintains that the processor must be a “separate legal entity with respect to the controller”.⁹⁹ Notwithstanding the fact that natural persons clearly may qualify as processors under Article 4(8), the assumption seems justified with respect to situations where entities are processing personal data on behalf of the controller. In the explanatory memorandum to the DPD, the Commission remarked that the controller may have personal data “processed by members of his staff or by an outside processor, a *legally separate* person acting on his behalf”.¹⁰⁰ Thus, individuals employed by the controller are not deemed processors, even if they process personal data on behalf of the controller. The rationale behind this is explained by neither the Commission nor by legal literature. However, there is an argument that employees and board members, by their own definition, act on behalf of the entity employing them. Any obligation imposed on the entity as a controller or processor would thus deem it responsible for the actions performed by its employees in relation to processing.

2.5.2 Persons “acting under the authority” of the controller or processor

The Regulation distinguishes processors from persons “acting under the authority of the controller”. While the latter phrase lacks a legal definition under the GDPR, it appears in Article 29, which stipulates that such persons should only process personal data on “instructions from the controller”. Article 4(10) stipulates that “third party” does *not* encompass the “processor” or “persons who, under the direct authority of the controller or processor, are authorised to process personal data”. Thus, processing by such persons is lawful as long as they act on instruction from the controllers. Employees clearly fall within this definition.¹⁰¹ In the case of external consultants and contractors, the distinction is important as the Regulation imposes far-reaching obligations on the controller with respect to utilization of processors.¹⁰²

As an example, an IT bureau could hire out an employee to an entity determining the purposes and means of certain processing activities. The consultant would work at the controller’s premises, and only process personal data on instruction from the controller. The question here is whether the IT bureau or the consultant would be a processor, or whether the consultant would be a person acting under the authority of the controller.

⁹⁹ WP 169 p. 25.

¹⁰⁰ COM(92) 442 final p. 10.

¹⁰¹ Büllesbach et al. (2010) p. 85. See also Van Alsenoy (2016) p. 79.

¹⁰² See, for instance, Article 28(3) GDPR, which requires processing by processors to be governed by a legal act or contract.

The word “authority” refers to “the power or right to give orders, make decisions, and enforce obedience”.¹⁰³ As the controller would have the power or right to give orders to both employees and processors, the wording provides minor guidance. The Norwegian language version refers to “*handler for*”, implying an action “on behalf of”. The Greek version mentions “*που ενεργεί υπό την εποπτεία*”, referring to a “person under supervision of”, while the German language version refers to an “*unterstellte Person*”, thus indicating a subordinate relationship. With respect to the processor, the controller would only have the right to give orders concerning the processing of personal data. Towards the employee, the mandate of instruction is far more wide-reaching. Olsen argues that the mandate of instruction, for instance through an employment contract, is decisive when distinguishing between a processor and a person acting under the authority of the controller.¹⁰⁴

In addition, the controller would normally be liable for actions performed by the employee, without any data processor agreement. The rationale behind operating with “processor” under the DPD was to “ensure that the protection of the data subject is not deleted where processing is carried out by a third party on the controller’s behalf.”¹⁰⁵ Considering this object, the persons “acting under the authority of the controller or processor” should only cover individuals subject to identification with the controller and for whom the controller has a legal responsibility.¹⁰⁶ Separate legal entities or external consultants would normally be contracting third parties, typically hired by the controller to perform specific services. As these bodies are not automatically identified with the controller, additional obligations like data processing agreements should be in place to ensure the rights and freedoms of data subjects.

103 Oxford dictionaries (2018).

104 Olsen (2015) p. 281.

105 COM(92) 442 final p. 34

106 Blume (2015) p. 295 argues that “data responsibility must rest on the entity” and that rules governing the relationship between the employer and employee should be determined by labour and tort law.

3 Identifying the controller and processor in practice

3.1 Introduction

The purpose of this chapter is to apply the established conditions for identifying the controller and processor in practical scenarios. The identification of controllers, joint controllers and processors may be apparent in certain cases, but various degrees of control, influence and collaboration concerning processing often complicate the assessment.

As this analysis seeks to allocate responsibilities in grey areas, the starting point is situations where it is unclear whether entities act as controller or processor. The practical scenarios subject to analysis involve franchise contractual relationships, consultant services, and social networking services. As there are considerable variations in the factual circumstances from case to case, the thesis discusses specific type cases.

3.2 Franchise contractual relationships

3.2.1 Concept and roles

By franchise, this thesis refers to contractual relationships where a franchisor allows a franchisee to exploit its trademark for a specified remuneration.¹⁰⁷ The franchisee will normally be a separate legal entity from the franchisor, and thus largely maintain its autonomy.

The franchisee and the franchisor may perform various processing operations for various purposes. Normally, they will each process personal data about their employees, contractors, and customers. This analysis will focus on processing where there is some degree of collaboration between the franchisor and franchisee, as those scenarios give rise to uncertainties.

The franchise contract may impose certain obligations on the franchisee such as collecting and disclosing personal data about customers. Personal data including name, address and contact information could be collected to run marketing operations centrally, while personal data regarding transaction history could be

¹⁰⁷ The Economist (2009).

processed to analyse customer behaviour, which in turn may provide the opportunity to perform behavioural advertising.

Other scenarios concern the handling of bookings and requests from customers through an online portal where the franchisee under the contract is obligated to participate. The processing may include collection, disclosure and use of a customer's personal data, where the franchisee and franchisor manage different parts of the "chain" of processing operations. An example of this is the booking platform provided by the InterContinental Hotels & Resorts franchise.

The following section will identify controllers and processors in the type of cases as mentioned in the previous two paragraphs.

3.2.2 Marketing operations in franchises

This section analyses the following scenario. The franchisor Elbuy Sweden ("ES") franchises its trademark to legal entities wishing to sell electronic products to consumers. Pursuant to the franchising contract, the franchisee is obliged to collect personal data from customers buying the products in-store and store it on a centralised database managed by ES.

Case 1

Through the database, ES processes the personal data for analysis and marketing purposes, deeming it the processing of personal data in this case. A customer wishes to access his personal data and contacts the Swedish data protection authority for guidance on where to send his enquiry.

The first step is to identify the party determining the purposes and means of that processing of personal data pursuant to Article 4(7) GDPR. ES obligates the franchisee to process the personal data and determines the means of that processing. Thus, the clear point of departure is that ES is the controller. The processing of personal data occurs *because* ES wants to strengthen its brand by performing marketing operations, and *by* utilizing its online database. Therefore, ES has the decisive influence over the personal data processed and is liable to affect the rights and freedoms of the data subjects. As ES manages the database, it would also be in a position to enforce the rights of the data subjects.

The franchisee is contractually obliged to process the personal data, seemingly without any autonomy in determining the purposes or means of the processing. Thus, it is the processor under Article 4(8) GDPR because it processes the personal data on behalf of ES. This is however just a starting point, and one may be

confronted with scenarios where controller responsibility, either joint or individually, is imposed on the franchisee.

Case 2

The franchisee may process the personal data of its customers for its own marketing purposes. This could be accomplished by having access to the online database and thereby targeting advertising to the registered customers. By having recourse to this tool, the franchisee is arguably participating in the determination of purposes and means of the processing of customer data, in line with the Court's judgement in C-210/16. The franchisee plays a predominant role in this marketing operation and decides whether such operations shall be performed. With access to the personal data of the registered customers, the franchisee would also be in a position to enforce the rights of the data subjects, although it might be restricted from fulfilling certain requests, such as erasure¹⁰⁸, pursuant to the franchising contract. However, as the Advocate General stated, complete control is not a fundamental necessity for imposing joint controllership.¹⁰⁹ Further, as the franchisee and the franchisor would "pursue closely related objectives"¹¹⁰, namely marketing of the trademark, the entities should be deemed joint controllers.

Case 3

To complicate the picture, in a situation where the franchisee is contractually obliged to perform marketing operations on behalf of ES by processing the customer data in question, in contrast to the first scenario, the franchisee would now be responsible for carrying out marketing by whatever means it saw fit. The franchisee will not have any autonomy in determining *whether* processing activities are to be performed other than cancelling the franchise contract. However, in C-210/16 the Advocate General pointed out that "[t]he view cannot [...] be taken that a person who may do no more than accept or refuse the contract cannot be a controller".¹¹¹ Thus, a franchisee accepting a non-negotiable contract may still be deemed a controller "given his actual influence over the means and purposes of the data processing".¹¹² The franchisee chose to enter into the contract with ES. Further, the actual processing and marketing are performed by the franchisee, which thus is liable to affect the rights and freedoms of the data subjects. Bearing the general objective of the provision in mind, which is to provide a clear allocation of responsibilities under the Regulation,

108 Article 17 GDPR allows data subjects to obtain erasure of their personal data on certain conditions.

109 See section 2.4.2.

110 Advocate General's opinion in C-210/16 paragraph 59.

111 Ibid. paragraph 60.

112 I.c.

the conclusion in this case is that the franchisee is a joint controller with the franchisor.

Case 4

Another question concerns controller identification where the franchisee processes personal data to pursue a different purpose defined by him. For instance, this could be a case where the franchisee discloses customers' personal data to third parties by utilizing its access to the database. The franchisee would clearly be the party determining the purposes of those processing operations and, because the purposes are separate, they constitute a different processing of personal data than those discussed above. As the franchisee decides which categories of personal data to be processed, and the tools used for that processing, he would also have a dominant influence in determining the means. Thus, the franchisee would be a controller for this processing of personal data. However, this then raises the question of the role of ES with respect to this processing.

By managing the online database, ES would clearly be processing personal data. However, it does not determine the purposes of this particular processing. The processing is in the interest of the franchisee which, in principle, deems ES the processor. As a starting point, joint control is precluded as there is no common determination of the purposes. This illustration shows that two parties may act respectively as controller and processor in relation to each other, in light of different sets of processing operations. In this particular case, one may ask if ES exercises so much influence in respect to determining the means of the processing that it would be deemed a joint controller.

Merely managing the online database does not make ES the determining party with respect to the means of the processing. The Regulation allows the processor some margin of manoeuvre concerning the determination of technical and organisational means.¹¹³ However, ES manages the online database containing customers' personal data. Based on this fact, one may argue that the franchisor exercises comprehensive influence with respect to deciding the storage time for the personal data, and the parties that have access to it. By having access to the personal data, it would also be in a position to enforce the rights of the data subjects. Another point, emphasised by the Court in C-210/16, is the fact that the franchisor, by managing and operating an online database containing customers' personal data, gives the franchisee the opportunity to process the customers' personal data.¹¹⁴ All these elements point towards the fact that the franchisor is liable to affect the rights and freedoms of the customers by influencing the

¹¹³ See section 2.3.2.

¹¹⁴ Paragraph 35.

means of the processing to a large extent. Thus, in a scenario as described, the franchisor is identified as a joint controller with respect to the processing of personal data for disclosure to third parties.

3.2.3 Shared platform for customer management

Some franchises operate with a common online platform for making and managing bookings. For instance, when booking a hotel through the InterContinental Hotels & Resorts franchise, the customer is required to create an online profile, and to fill in name, e-mail address, profession and country/region.¹¹⁵ This information is subsequently disclosed to the relevant franchisee, which undertakes further administration of the reservation.¹¹⁶ This chapter will identify the controller and processor with respect to processing of personal data through such online platforms.

For processing of personal data for marketing purposes and loyalty programs, the franchisor would be the controller as it determines those purposes and the means to achieve them. However, this analysis focuses on processing of personal data for the purposes of managing the reservation of a hotel room. The processing performed would be the collection, disclosure and use of personal data. As the operations share the same purpose, they are regarded as one processing.¹¹⁷ Who determines the purpose and means of this set of operations pursuant to Article 4(7) GDPR?

One could argue that the franchisor is a processor with respect to the franchisee as it processes the personal data for the franchisee's purposes, namely making possible the reservation of a hotel room at the franchisee's premises. It is, however, doubtful whether the franchisor processes on the franchisee's *instructions*¹¹⁸. Naturally, the franchisee may end the processing by cancelling the franchise agreement. However, the franchisor maintains its autonomy in deciding the personal data to be processed, for how long it is to be kept, and the persons/bodies to have access to it. This indicates that the franchisor is a controller in its own right, substantiated by the influence over the processing operations, and by being able to enforce the rights of the data subjects.

These facts lead to the question of whether the franchisor and franchisee jointly determine the purposes and means of the processing of personal data through the online booking portal. Where two entities together decide to create and manage an online platform service for sharing customers' personal data and

115 <https://www.ihgplc.com/en/subscriptions/subscribe>

116 https://www.ihg.com/content/gb/en/customer-care/privacy_statement

117 See section 2.2.2.

118 See section 2.5.1.

managing customer requests, the entities would clearly be determining the purposes and means of the processing operations relating to the use of the portal.¹¹⁹

However, in this case, there does not seem to be any joint determination of the means and purposes. The franchisee would normally be obliged to let the franchisor perform its processing operations in order to exploit the trademark. Further, the franchisee would have little or no influence with respect to the personal data processed on the portal.

Against this background, an argument is that the set of processing operations should be delineated at micro level.¹²⁰ Based on factual influence, the franchisor would have complete control over the processing operations performed until the personal data is disclosed to the franchisee. At this moment, the franchisee would have influence and control over the personal data. Rather than assuming joint control under the GDPR, the transfer of personal data between the parties may be considered a collaboration between two single controllers. As the parties have limited influence over the processing of personal data performed by the other party, this solution seems reasonable.

3.3 Consultant services

3.3.1 Concept and roles

This thesis defines “consultant services” as contractual relationships where a customer contracts or hires another entity or individual to perform a defined service for the customer. Typical consultant services include assistance regarding legal advice, accounting, and engineering.¹²¹ Such consultants could be entities specializing in certain professions, entities where the primary business is staff contracting, or merely individual consultants.

This section identifies the controller and processor where processing of personal data is performed by a consultant hired to perform a specified service for the customer. The processing operations regarding the respective entities’ own employees and marketing are not problematic and thus not assessed.

3.3.2 Legal consultants

Undertakings or individuals as clients may approach legal consultants for legal guidance or representation during a trial. Such work would normally require

119 WP 169 p. 20.

120 See section 2.4.2.

121 ICO (2014) paragraph 26.

collection, storage and use of personal data. However, undertakings offering legal services may also provide other services such as audits.¹²² The identification of controllers and processors may be different with respect to the content of the service.¹²³ For instance, an accountant engaged by a firm to carry out an audit is normally considered a processor, while the firm is a controller.¹²⁴

However, this analysis presupposes a traditional legal service, and assumes the following facts. The Werner Brethren company (“the client”) hires the law firm Melsom & Sons (“MS”) to identify and sue individuals infringing client-owned copyrighted content by sharing video files through a peer-to-peer network. Later, one of those individuals receives a compensation claim and decides to contact the client in order to gain access to his or her personal data. The client dismisses the request by claiming it is not the controller. The question here is whether this contention is sustainable.

The client decides to enter into an agreement with MS and determines the purpose of the processing, namely mapping individuals infringing copyrighted content. Thus, one may argue that the client is the controller. Further, MS would arguably perform its services on behalf of the client, and thus be a processor. The processing is being performed for the client’s purposes and the client has the mandate to end it. The majority of the Norwegian Data Protection Tribunal maintained this view in case PVN-2011-10.¹²⁵ However, legal scholars have argued that legal consultants are *not* processors with respect to their clients. It is maintained that such consultants “work independently and would never allow their clients to decide how data is handled (for instance, processed and archived) in the lawyers office.”¹²⁶ Furthermore, the legal consultant decides what personal data is to be processed and “controls the detailed content of the advice”.¹²⁷ WP29 argues that “the traditional role and professional expertise of the service provider [...] may entail its qualification as a data controller.”¹²⁸

Having a predominant role in deciding how the data should be processed is indeed a strong argument for imposing controller responsibility on legal con-

122 For instance, Deloitte offers, inter alia, legal advice, audit and consulting services (see <https://www2.deloitte.com/global/en/pages/about-deloitte/articles/about-deloitte.html>).

123 As an illustration, see Rt-2014-773 where the Norwegian Supreme Court discussed whether an attorney performing an investigation to uncover illegal actions in an entity performed a *legal service*.

124 WP 169 p. 29.

125 To the contrary, the minority concluded that the law firm was the controller by placing decisive emphasis on its autonomy in determining the means of the processing.

126 Büllesbach et al. (2010) p. 38.

127 ICO (2014) paragraph 27.

128 WP 169 p. 28.

sultants.¹²⁹ With regard to this case, MS decides the what, how and who with respect to the processing of personal data. Also, in relation to the client, MS would determine the personal data required to provide their service. Furthermore, personal data would normally be stored and processed at the legal consultant's premises. Thus, MS has the power to influence the processing of personal data in accordance with the GDPR. The consultant would also be in a position to enforce the rights of the data subjects. Even though it does not determine the final purpose of the processing operations, the legal consultant would have so much autonomy in deciding the means of the processing that it would be the controller with respect to those processing operations.¹³⁰

Against this background, one may argue that the client is either a controller in its own right, a joint controller with MS, or not a controller at all. The client certainly has influence over the processing of personal data, as it could end it at any time. Further, the determination of the purpose of the processing (pursuing copyright infringers) lies explicitly with the client. A counter-argument against controller responsibility is the fact that the client lacks influence with respect to compliance with the GDPR and lacks the possibility to enforce the rights of the data subjects. Still, it is impossible to avoid the fact that the client determines the purposes of the processing pursuant to Article 4(7). Thus, keeping in mind the fact that a joint controller is not required to have control over every aspect of the processing, the client is a joint controller with respect to the processing operations performed to achieve its purposes. As the Advocate General stated, it is "precisely for that type of situation [the DPD] expressly provides that control may be exercised jointly".¹³¹ It is also an argument, in light of the Court's decision in C-210/16, that the client, by contracting MS, gives MS the opportunity to process personal data. Thus, the client is a joint controller with MS, and must ensure enforcement of the rights of the data subject pursuant to Article 26(3) GDPR.

3.3.3 Hired consultants

The following assessment seeks to elucidate the distinction between a processor and a person acting under the authority of the controller ("PUAC"). As it would be impractical to discuss all possible scenarios where individuals are hired for various purposes, this evaluation will focus on the following three types of cases: contracting, temporary appointment, and staff contracting.

¹²⁹ C-131/12 paragraph 36.

¹³⁰ Carey (2018) p. 182 establishes that the degree of autonomy regarding the processing is the "distinguishing feature between a processor and a controller".

¹³¹ The Advocate General's opinion in C-25/17 paragraph 71.

Typically, individuals classified as an “employees” are within the scope of PUACs. However, as the definition of employees may vary between member states, simply linking PUACs to the definition of employees is not sufficient.¹³² As assessed in section 2.3.2 of this thesis, the mandate of instruction and identification between the employees and the controller is relevant criteria for assessing the distinction between processors and PUACs. In essence, one should ask whether the obligations under the GDPR towards processors ought to be imposed on the employees/contractor to ensure complete and effective protection of the data subjects.¹³³

Contracting

One side of the scale concerns *contracting*, where an entity or individual engages a firm to perform a specific service or a job, for instance IT services. The firm providing the service is defined as a contractor, and the individuals performing the service are employees of the contractor. Contracting is typically characterised by employees acting under the contractor’s mandate of instruction rather than the hiring entity. Further, the contractor is normally subject to independent liability for its performance and the task is clearly defined.¹³⁴

Should contracting services require processing of personal data, the engaging entity would be the controller as the processing would be performed on behalf of it. With regard to the individuals performing the task, they would not be acting under the authority of the controller because they are subject to the contractor’s mandate of instruction. In addition, the latter would have independent liability for the individual’s actions. As there is identification between the contractor and its employee, the contractor would be a processor and the individual a person acting under the authority of the *processor*.

Temporary employment

At the other side of the scale, there are situations where a controller temporarily hires a stand-in to cover for an employee and its tasks include processing of personal data. The stand-in would be subject to the controller’s mandate of instruction through an employment contract as the controller acts as an employer towards the employee, regardless of the fact that the employee also may have a contract of employment with a temporary work agency. The liability for the performance normally lies with the hiring entity, and the tasks to be performed are vague or undefined than they are under contracting agreements.¹³⁵

132 For instance, directive 2001/23/EC (OJ L 82 22.03.2001 p. 16–20) Article 2(1)(d) allows member states to establish the definition of an “employee”.

133 See section 2.5.2.

134 NOU 1998:15 section 5.1.4.

135 I.c.

The controller would have a wide mandate of instruction towards the stand-in, and normally be liable for its actions. In addition, the stand-in would have no autonomy with respect to the processing. Thus, the stand-in would not be a processor, but a PUAC. Thus, the controller and stand-in would not be subject to obligations with respect to use of processors.

Staff contracting

Between these situations, the assessment may be more unclear. As an illustration, the Norwegian Supreme Court discussed whether an individual performing tasks related to mail handling at Statoil's premises was engaged as a hired employee through a labour contracting agency, or as part of a contracting service. The Court found that the individual did not have any contract of employment with Statoil, that his tasks were clearly defined between Statoil and the labour contracting entity, and that the latter had liability for the tasks performed. The Court thus concluded that the individual acted as part of a contracting agreement, rather than staff contracting.¹³⁶

Considering the fact that the individual processed personal data on behalf of Statoil, the latter would clearly be a controller in the described case. However, a question is whether the employee performing the task would be a processor, a person acting under the authority of Statoil, or a person acting under the authority of the labour contracting entity. Statoil's mandate of instruction was limited to instructions regarding the specific task at hand. There was no identification between the employee and Statoil. Rather, the recruitment agency was found to be liable for the actions of the employee vis-à-vis Statoil. The labour contracting entity should thus be regarded as a processor in this case. Since the employee was subject to a contract of employment with the labour contracting entity, he was considered a person acting under the authority of that entity, which would be the processor.

The assessment might have had a different outcome if Statoil had engaged the employee to perform vague or undefined tasks. Had the employee signed a contract of employment with Statoil, the duties of the employee would be an obligation of best efforts, subject to Statoil's mandate of instruction. Then, Statoil could have instructed the employee directly, without authorisation from the labour contracting entity. Further, Statoil would normally be subject to identification with the employee, and liable for its actions. Against this background, the rights of the data subjects and obligations imposed on Statoil under the GDPR are sufficiently safeguarded without imposing processor responsibilities on the

136 Rt-2013-998. The dispute in question concerned labour law.

employee. In this scenario, Statoil is not obliged to enter into a data processing agreement with either the employee or the labour contracting entity.

3.4 Social networking services

3.4.1 Concept and roles

For the purpose of this thesis, “social network service” means interactive web and application platforms enabling individuals/groups to create user-specified profiles, generate content, and connect with other individuals/groups.¹³⁷ The main actors in social networking services are the social network provider (“SNP”) and the individual or group as a *user* of that social network service.

The performance of personal data processing in social network services happens for various purposes. For the SNP, personal data is normally processed to manage, run and enhance the social network service, and especially to perform targeted advertising.¹³⁸ For the users, processing operations consist of uploading content, interacting with other users and, in some instances, offering services and advertisements for businesses (for instance, through fan pages).

Van Alsenoy has analysed the allocation of controller responsibilities in online social networks.¹³⁹ While this thesis considers his analysis, independent conclusions are made, especially taking case C-210/16 into account.

The processing of personal data for managing, enhancing and performing targeted advertising on a social network could consist of the collection and disclosure of personal data about users, especially name, age, relationship status, employment status, and activity on the social network. As the SNP autonomously determines both means and purposes for these processing operations, the SNP would clearly be the controller pursuant to Article 4(7) GDPR.

As this chapter seeks to assess the grey areas, the further assessment will focus on controller identification with respect to user-generated content.

3.4.2 User-generated content

With respect to user-generated content, the processing of personal data could amount to uploading photos, publishing information and sharing personal data of other data subjects. This section assesses the processing of personal data per-

¹³⁷ Obar and Wildman (2015) p.746-747.

¹³⁸ Rich (2011).

¹³⁹ Van Alsenoy (2016) p. 352-361.

formed to achieve this purpose. This analysis assumes the following facts. A Facebook-user, Magnus, decides to upload a publicly available photo of his colleague Karoline's empty office, supplementing it with a text stating she has been away from work due to illness. When Karoline finds out, she contacts Facebook and demands her personal data be removed from the platform. In its response, Facebook refuses to remove the post, claiming Magnus is the controller pursuant to Article 4(7) GDPR. In this case, the question is whether this statement is legally valid.

It is important to note that the GDPR is not applicable to processing "by a natural person in the course of a purely personal or household activity" (see Article 2(2)(c)). In general, the derogation does not apply when personal data are published on the internet and thus "made accessible to an indefinite number of people".¹⁴⁰ Its scope of application could be in situations where the personal data are only accessible to a very limited group of individuals, or for activities such as "correspondence and the holding of addresses".¹⁴¹ However, as the personal data uploaded in this case is publicly available, the "household exemption" does not apply.

When Magnus uploads content containing personal data on others, he determines the purpose of that processing operation. As for the means, Magnus determines what personal data is disseminated and for how long the personal data is publicly available. Facebook also allows Magnus to specify the persons who have access to the personal data on the social network. Thus, Magnus clearly determines the essential means¹⁴² of the processing of personal data carried out and is a controller in relation to that processing.

The role of Facebook with respect to this processing is more difficult to assess. Van Alsenoy outlines several opinions by scholars regarding the matter.¹⁴³ One solution is that Facebook is merely a processor, as it does not hold any control over the content uploaded by Magnus.¹⁴⁴ Indeed, it could be argued that through its platform, Facebook processes personal data on instruction from Magnus, and to achieve his purposes. The fact that Facebook provides for the technical and organisational measures exploited by Magnus could lie within the part of the "means determination", which could be delegated to the processor. There are, however, strong counter-arguments to this point of view. First, Facebook

140 C-101/01 paragraph 47. The judgement concerned the equivalent provision under the DPD.

141 Recital 18 GDPR holds that such activities on social networks are covered by the household exemption.

142 See section 2.3.2.

143 Van Alsenoy (2016) p. 353-355

144 Van Eecke and Truyens (2010) p. 538

would have extensive autonomy in determining the means of the processing, especially concerning security and the location of personal data.¹⁴⁵ Second, Magnus, rather than Facebook, would be responsible for processing in compliance with the data protection principles under the GDPR. He would have limited influence with respect to compliance and ensuring the rights of the data subject. As a third argument, it could prove to be impractical if all users must enter into a data processor agreement with an SNP.

A second possibility is that Facebook and Magnus act as joint controllers, implying they jointly determine the purposes and means of the processing of personal data. This line of argument builds on the fact that Facebook determines the purposes and means of the social network as a whole, and that the processing concerning user-generated content is part of the service offered by the SNP.¹⁴⁶ This viewpoint is underlined by the Advocate General in C-210/16, where he maintained that Facebook “principally decided on the purposes and means” of the data processing in question “as the designers” of that processing.¹⁴⁷ Even though Facebook cannot control the content uploaded by Magnus, it is the service provider and thus able to remove it. As such, it is significantly liable to affect the rights of the data subjects.

Assuming joint controller responsibility would best ensure the effective protection of the data subjects. Facebook and Magnus would be directly obliged to ensure compliance with the data protection principles while Karoline, in principle, could exercise her rights under the GDPR towards both Facebook *and* Magnus.

145 This argument was maintained in the SWIFT case (see section 2.3.2.)

146 Van Alsenoy et al. (2009) p. 70-71.

147 Advocate General’s opinion in C-210/16, paragraph 47.

4 The suitability of the controller/processor distinction

4.1 Introduction

A radical change pursuant to enacting the GDPR was the number of obligations imposed directly on the processor. Contrary to the DPD, the Regulation imposes duties *inter alia* to cooperate with national supervisory authorities¹⁴⁸, maintain records of processing activities¹⁴⁹, and implement technical and organisational measures¹⁵⁰. More significantly, processors are directly subject to sanctions and compensation claims under the GDPR.¹⁵¹ The obligations imposed on the processor may have been the European legislators' attempt to handle technical development and chains of sub-processors processing personal data on behalf of the controllers. Indeed, the Commission argued that imposing legal obligations on processors would “ensure that that outsourcing and delegation by controllers to processors do not result in lowering the standard of data protection”.¹⁵²

148 Article 31 GDPR.

149 Article 30(2) GDPR.

150 Article 32 GDPR.

151 Carey (2018) p. 178. See Articles 82-83 GDPR.

152 SEC(2012) 72 final p. 109.

Relevant provisions	Directive 95/45	GDPR
<i>Applicable law</i>	X	✓
<i>Principles of data quality</i>	X	X
<i>Legitimacy of processing</i>	X	X
<i>Sensitive data</i>	X	X
<i>Transparency</i>	X	X
<i>Data subject rights</i>	X	Applicable through contract (exceptions)
<i>Co-operation with supervisory authority</i>	Implied	✓
<i>Data protection by design and by default</i>	X	X
<i>Documentation</i>	Not specified	✓
<i>Confidentiality</i>	✓	✓
<i>Security</i>	Applicable through contract	✓
<i>Data breach notification</i> ¹²⁰⁰	X	✓
<i>DPIA, prior authorization</i>	X	Applicable through contract (exceptions)
<i>Data protection officers</i>	X	✓
<i>Codes of conduct, certification</i>	Not specified	✓
<i>International transfers</i>	Not Specified	✓
<i>Liability</i>	X	✓
<i>Administrative fines</i>	Not Specified	✓

Table 1: The obligations imposed on processors under the GDPR that are contrary to the DPD. Borrowed from Van Alsenoy (2016) p. 269.

Blume argues that the imposition of duties on the processor may undermine “the general structure of data protection law”.¹⁵³ For instance, the controller may

¹⁵³ Blume (2013) p. 144.

lean against the fact that the processor is obliged to implement appropriate security measures (see Article 32 GDPR). Still, controllers may only use processors “providing sufficient guarantees” regarding security measures (see Article 28(1) GDPR). Others have indicated that the obligations imposed on processors are somewhat arbitrary. For instance, the obligation to enforce the rights of data subjects are imposed solely on the controller, but supervisory authorities may still demand access to all personal data and information from the processor pursuant to Article 58(1) (e).¹⁵⁴ Further, processors are not required to implement “privacy by design and default” pursuant to Article 25 GDPR. Thus, processors are not accountable for breaches of this obligation, even though they often decide on technical measures with respect to the processing.

There are still justifiable reasons for extending obligations to the processors. Their growing role in the determination of the means of the processing (for instance, cloud service providers) substantiates a need for greater accountability for such operators.¹⁵⁵ From the data subject’s point of view, he or she may claim compensation directly from the processor in the case of breach of the Regulation, and he or she is “protected against insolvency of any of the parties involved in the processing”.¹⁵⁶

One may still ask why the European legislators decided to retain the distinction between controller and processor, and only impose some obligations on the latter. The next section will assess whether the distinction between controller and processor is necessary in light of the developments in data protection law and the society as such.

4.2 Eliminating the processor

Pursuant to the enactment of the GDPR, legal scholars proposed removal the concept of processors from the Regulation because of the “increasingly blurred [distinction] in an interconnected world of ubiquitous computing”.¹⁵⁷ Against this background, de Hert and Papakonstantinou argue that the Commission should “boldly abolish the notion of data processors” and impose controller responsibility on the person or entity processing personal data without giving any regard to purposes and means. Blume agrees, and holds that “sole and exclusive responsibility”¹⁵⁸ under data protection law should be imposed on the entity

154 Treacy (2012) p. 3-4.

155 EDPS (2013) paragraph 25.

156 Van Alsenoy (2016) p. 511.

157 De Hert and Papakonstantinou (2012) p. 134.

158 Blume (2015) p. 295.

actually processing personal data. Taking the object of operating with processors into consideration, one may ask whether the application of “processors” under the Regulation really secures the data subjects’ rights when processing operations are outsourced to third parties.

As the ICO¹⁵⁹ pointed out, pursuant to the “collaborative nature of modern business, it is rare for one organisation (the processor) to only act on instructions from another (the controller)”.¹⁶⁰ The ICO substantiates this by the fact that the processor enjoys great autonomy in the performance of its services for the controller and the “complex collaborative arrangements involving numerous organisations”.¹⁶¹ This lack of clarity may indeed pose a threat to the rights of data subjects when processing operations are outsourced. Underlined by recent case law and discussions regarding social network providers and cloud providers, data subjects may indeed face difficulties regarding what entity they may exercise their rights towards. It may also be unclear what entity is primarily responsible for compliance with the principles of data protection.

Another objective of distinguishing between the controller and processor was to provide for legal certainty.¹⁶² The blurred distinction may result in considerable uncertainties for entities assessing their obligations and risks. Principally, a controller would remain liable for data protection breaches by processors where the actual control over the processing is limited.¹⁶³ This is especially relevant given the developments in the use of sub-processors and chains of such sub-contractors for processing operations. Further, Van Alsenoy argues that abolishing the distinction would eliminate an “artificial construct that has given rise to considerable difficulties of interpretation”.¹⁶⁴ Indeed, the SWIFT case proves that time and effort spent on determining controller or processor responsibility is often excessive, and that resources could be allocated to “more substantive compliance requirements”.¹⁶⁵

The fact that the distinction is unclear does not necessarily mean that removing the concept of “processors” would enhance the protection offered to individuals. Upon enactment of the GDPR, an external report stated that equal distribution of responsibilities to all entities processing personal data would not take “into account their individual position, the scope of their tasks, or the expectations of

159 The ICO (Information Commissioner’s Office) is the UK data protection authority.

160 ICO (2013) p. 34

161 I.c.

162 See section 2.5.2.

163 Moerel (2012) p. 216-217.

164 Van Alsenoy (2016) p. 509.

165 Bird & Bird p. 4.

data subjects.”¹⁶⁶ In other words, an over-simplistic approach may decrease legal certainty and impose obligations on actors disproportionate to the task they are performing.

Van Alsenoy emphasises the processor-controller relationship as a normative concept, indicating “what the relationship *should* look like”.¹⁶⁷ The GDPR rests on the concept that controllers define the purposes of processing operations, while processors merely act to achieve that purpose. Should any data processing entities be controllers in their own right, they might be less reluctant to further process personal data for their own purposes. Notwithstanding this fact, the requirements of legal grounds and other principles of data processing would still apply to the entity.

A third counter argument relates to transaction costs. By removing the concept of processors and allocating all data protection obligation to any person involved in the processing of personal data, each entity would have to ensure compliance with the Regulation as a whole. The establishment of legal grounds for processing data, information to data subjects and regimes to enforce data subject rights would have to be assessed by each entity. Rather than allocating the full costs and risks to one principally responsible entity, costs would be directed to every actor involved in the processing of personal data.¹⁶⁸

4.3 Allocating responsibilities to the initiating party

Linking controller responsibility to the determination of “purposes and means” has been criticised by scholars. For instance, the word “and” indicates that *both* purposes and means must be determined by one party in order for that party to be deemed a controller. As a practical solution, WP29’s distinction between essential and non-essential means¹⁶⁹ may be fitting in some situations, but not in others. Considering the fact that the determination of technical means may deem a service provider liable to affect the protection of the data subjects, it is not always clear that this entity should be a processor and not a controller. The interpretation is also contrary to the wording of Article 4(7) and changes the word “and” to “or”.¹⁷⁰

166 Konarski et al. (2012) p. 31.

167 Van Alsenoy (2016) p. 510. Author’s italicisation.

168 Ibid p. 511.

169 See section 2.3.2.

170 Van Eecke and Truyens (2010) p. 539.

Rather than removing “means” from the definition, the European Commission proposed to add “conditions”, meaning the controller would be the body determining “the purposes, *conditions* and means of the processing”.¹⁷¹ However, the proposal was heavily criticised¹⁷² and amended by the European Parliament.¹⁷³ Thus, there is no reference to conditions of the processing under Article 4(7) GDPR. However, in its response to the Commission’s consultation on enacting the GDPR, the ICO suggested that controller responsibility should be imposed on the

organisation, or organisations, that *initiate* the processing, whereas anyone processing personal data at any stage of the information life cycle should be responsible for dealing with it properly and securely and be accountable for their own aspect of the processing.¹⁷⁴

The proposal is interesting as there will always be a party initiating processing of personal data. Further, the *initiation* of processing activities is not too radical a change from today’s Regulation. However, the question would still be *why* the processing is taking place.¹⁷⁵ The initiating party would be responsible for all processing stemming from its decision to initiate it, while processors are only accountable for the processing in which they are involved.

Van Alsenoy recognises the solution, as the data subject would always have the opportunity to “seek remedy from a single actor in relation to every aspect of the processing”¹⁷⁶. Further, it removes the “possibility for service providers to ‘hide’ behind their processor status”. Besides, it is arguably easier to determine the party or parties initiating a processing operation than handling the complicated concepts of “purposes and means”.

It is, however, questionable whether this solution would provide any clarification. It is unclear what obligations parties accountable for their “own aspect” of the processing would comply with. If all obligations under the GDPR, including enforcing the rights of data subjects, are imposed, the solution would be no different than assessed in chapter 4.1.2, where each party involved in processing of

171 COM(2012) 11 final p. 41.

172 Konarski et al. p. 30 holds that implementing “conditions” would raise “additional complications and doubts.”

173 PE501.927v04-00 p. 82-85.

174 ICO (2009) p. 2-3.

175 See section 2.3.2. The Article 29 Working Party explicitly recognises that the question “who initiated [the processing]?” is an element in assessing the party determining the purposes and means.

176 Van Alsenoy (2016) p. 513-514.

personal data is deemed a controller. Further, it would be difficult to assess controller responsibility where entities jointly initiate processing operations. Consider the fact that one collaborating party decides to perform the same processing as initiated by both parties, but for its own purposes. It would arguably be unreasonable for the other party to assume full responsibility and liability for this processing activity, even though it initiated the processing operation.¹⁷⁷

177 I.c.

5 Concluding remarks

5.1 Lex lata

It is necessary to allocate responsibilities for compliance with data protection law. By imposing those obligations on the body determining the means and purposes of a specific processing of personal data, the European legislators intended to allocate responsibilities to the body able to influence it.

The first question clarified the concept of “processing”. The concept is interpreted in a wide sense and encompasses any action performed on personal data. When distinguishing one set of processing operations from another, the purpose of the processing operations determines to what *one* processing of personal data refers.

The analysis further assessed the factual circumstances determining controller or processor responsibility. It is often unproblematic to identify the controller with respect to processing of personal data. In such scenarios, one entity clearly and autonomously determines *why* the processing is taking place, the personal data to be processed, and the parties that will have access to it. However, practice in recent years underlines the fact that controller designation is often more difficult.

If in doubt, the determination of controller responsibility must be assessed in light of the object of operating with controllers and processors. Controller responsibility is imposed on the body ultimately responsible for the choices governing the processing of personal data. Outsourcing of processing activities should never curtail the rights and freedoms of data subjects. The limited CJEU practice and opinions of the Advocate General substantiate this fact by interpreting “controller” broadly. Two key questions to ask are what entity is liable to affect the rights and freedoms of data subjects significantly, and what entity is in a position to enforce their rights.

When identifying the processor, one should, in essence, ask whether the entity processes personal data on instruction from a controller, and whether the processing activities are performed to achieve the purpose as defined by the controller. The GDPR allows the processor a certain degree of autonomy in deciding

the technical and organisational means of the processing, but too much autonomy may result in the supposed processor being a controller.

The notion of joint controllers is still a difficult concept under the Regulation. To assess whether two entities are joint controllers, one must look at each single processing activity and check whether both parties play a predominant role in the determination of purposes and/or means for *that* processing operation. The influence over the processing does not have to be equal; one joint controller may, for instance, determine the essential means of the processing, while the other determines the purposes.

5.2 Lex ferenda

Although the abolishment of the concept of processors may be a radical change, one cannot deny the fact that the European legislators missed an opportunity to provide further clarification on the concept of controllers and processors. Changes with respect to technology, organisational differentiation and globalisation will continue to develop for years to come, meaning further complications regarding processor and controller identification may emerge. The development of blockchain technology is especially of interest in relation to allocating responsibilities for data protection.¹⁷⁸

Irrespective of this, amendments to the definition of controller or abolishing the processor require a sufficient alternative. The alternative must better ensure the rights and freedoms of data subjects. Any change should also be sufficient to strengthen legal certainty for economic operators with respect to their obligations and liabilities. As of today, the current solution may very well be the best among the proposed solutions.

Considering the extended autonomy of certain service providers processing personal data in today's society, it is indeed an argument that the additional obligations placed on processors under the GDPR may have been a wise choice in protecting data subjects' personal data. The change is likely to provide for greater incentive for service providers to ensure compliance with the obligations in the future.

178 Hogan Lovells (2017) p. 10.

Bibliography

Treaties

TFEU	OJ C 326. Consolidated version of the Treaty on the Functioning of the European Union.
TEU	C 115/13. Consolidated version of the Treaty of the European Union.
Conv. 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Legislation

EU legislation

95/46/EC OJ L 281, 23.11.1995 p. 31-50	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
2001/23/EC OJ L 82, 22.3.2001, p. 16-20	Council Directive 2001/23/EC of 12 March 2001 on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses.
2016/679/EU OJ L 119, 4.5.2016, p. 1-88	Regulation of the European Parliament and 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).

National legislation

- 1978 French data protection act. *Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf> Last accessed 11/04/2018.
- 1988 Irish Data Protection Act (Consolidated version). http://www.lawreform.ie/_fileupload/RevisedActs/WithAnnotations/EN_ACT_1988_0025.PDF Last accessed 11/04/2018.
- 1997 Norwegian National Insurance act. *Lov om folketrygd (folketrygd-loven)*. (Lovdata)
- 2000 Danish data protection act. *Lov nr 429 af 31/05/2000 om behandling af personoplysninger*. <https://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/> Last accessed 11/04/2018.
- 2000 Norwegian data protection act. *Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)*. <https://www.datatilsynet.no/en/regulations-and-tools/regulations-and-decisions/norwegian-privacy-law/personal-data-act/> Last accessed 10/03/2018.
- 2003 German data protection act. *Bundesdatenschutzgesetz*. http://www.gesetze-im-internet.de/englisch_bdsch/ Last accessed 11/04/2018.
- 2005 Norwegian Working Environment act. *Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)*. <https://lovdata.no/dokument/NLE/lov/2005-06-17-62> Last accessed 24/04/2018.

Får feilmelding på denne linken. Både her og i Word-dokumentet

Case law

The European Court of Justice

Case C-101/01 Lindqvist	EU:C:2003:596
Case C-73/07 Tietosuoja valtuutettu	EU:C:2008:727
Case C-28/08 European Commission v The Bavarian Lager co. Ltd	EU:C:2010:378
Case C-131/12 Google Spain and Google Inc v Agencia Española de Protección de Datos and Mario Costeja González	EU:C:2014:317
Case C-201/14 Smaranda Bara and Others	EU:C:2015:638
Opinion of Advocate General Bot in Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH	EU:C:2017:796
Case C-434/16 Nowak	EU:C:2017:994
Opinion of Advocate General Mengozzi in Case C-25/17 Tietosuoja valtuutettu v Jehovan todistajat — uskonnollinen yhdyskunta	EU:C:2018:57
Case C-210/16 Wirtschaftsakademie Schleswig-Holstein	EU:C:2018:388
Case C-25/17 Jehovan todistajat	EU:C:2018:551

Others

PVN-2011-10	The Norwegian Data Protection Tribunal. <i>Simonsen - antipiratarbeid</i> . 2012.21.03 https://www.personvern.no/pvn-2011-10 Last accessed 25/03/2018.
Case of Various Claimants and Wm Morrisons Supermarket PLC	The British High Court of Justice, Queen's Bench Division. 2012.21.03. http://www.5rb.com/wp-content/uploads/2017/12/MORRISONS-approved-judgment.pdf Last accessed 05/04/2018.

Rt-2013-998	The Norwegian Supreme Court. A v Statoil ASA. (Lovdata)
Rt-2014-773	The Norwegian Supreme Court. A v Norsk Kylling AS. (Lovdata)

Preparatory works

The European Commission

COM (92) 422 final *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* <http://aei.pitt.edu/10375/1/10375.pdf> Last accessed 11/04/2018.

COM (95) 375
final-COD287 *Opinion of the Commission pursuant to article 189 b (2) (d) of the EC treaty, on the European Parliament's amendments to the council's common position regarding the proposal for a European Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51995PC0375&qid=1520606247647&from=EN> Last accessed 11/04/2018.

SEC (2012) 72 Final *Impact assessment.* <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN> Last accessed 11/04/2018.

COM (2012) 11
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)* <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN> Last accessed 11/04/2018.

The European Parliament

Konarski, Xavery
Karwala, Damian
Schulte-Nölke, Hans
Charlton, Shaun *Reforming the Data Protection Package* (2012). Study commissioned by the European Parliament, Directorate-General for Internal Policies. IP/A/IMCO/ST/2012-02. PE 492.431. Link Last accessed 11/04/2018.

P7_TC1-COD (2012) 0011 *Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No .../2014 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).* <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0212+0+DOC+PDF+V0//EN> Last accessed 10/03/2018.

PE501.927v04-00 2012/0011(COD). Amendments (2) 602 – 885. *Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* http://www.europarl.europa.eu/cmsdata/59683/att_20130508 ATT65808-8730162485448665006.pdf Last accessed 23/04/2018.

Council of the European Union

Doc. 5419/16 *Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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).* <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf> Last accessed 23/04/2018.

The European Data Protection Supervisor (EDPS)

EDPS *Additional EDPS comments on the Data Protection Reform Package (2013).* <http://www.statewatch.org/news/2013/mar/eu-edps-add-cooments-new-dp-reg.pdf> Last accessed 2018.25.03.

Reports and other documents

The Article 29 Working Party (WP29)

- WP 128 *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf Last accessed 11/04/2018.
- WP 169 *Opinion 1/2010 on the concepts of controller and processor*. Link Last accessed 11/04/2018.
- WP 203 *Opinion 03/2013 on purpose limitation*. Link Last accessed 11/04/2018.

National Data Protection Authorities

- The Danish Data Protection Authority *Guidelines on controllers and processors* (2017). Link Last accessed 20/03/2018.
- ICO *The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data* (2009). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/public_authorities/ico_uk_en.pdf Last accessed 23/03/2018.
- ICO *Proposed new EU General Data Protection Regulation: Article-by-article analysis paper* (2013). <https://ico.org.uk/media/about-the-ico/documents/1042564/ico-proposed-dp-Regulation-analysis-paper-20130212.pdf> Last accessed 02/04/2018.
- ICO *Data controllers and data processors: what the difference is and what the governance implications are* (2014). <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> Last accessed 02/04/2018.

Others

- Bird & Bird *Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/unregistered_organisations/bird_bird_en.pdf Last accessed 28/03/2018.
- The Danish Ministry of Justice Opinion no. 1565 on the General Data Protection Regulation – and the regulatory framework for Danish legislation (2017). Link Last accessed 01/03/2018.
- Korff, Douwe Brown, Ian *European Commission report on New Challenges to Data Protection* (2010). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1636706 Last accessed 02/04/2018.
- NOU 1998:15 The Norwegian Ministry of Labor and Government Administration. *NOU 1998:15 Arbeidsformidling og arbeidsleie* (1998). (Lovdata)
- Ot.prp. nr. 92 The Norwegian Department of Justice. *Ot.prp. nr. 92 (1998-99) on the Norwegian Data Protection Act (1998-99)*. <https://www.regjeringen.no/no/dokumenter/otprp-nr-92-1998-99-/id160088/sec1> Last accessed 11/04/2018

Legal literature

Books

- Büllesbach, Alfred
Gutwirth, Serge
Poullet, Yves
Prins, Corien
Concise European IT Law. 2nd edition. Kluwer Law International, 2010. Last accessed: 25/03/2018.
- Bygrave, Lee
Data Privacy Law – An International Perspective. 1st edition. Oxford University Press, 2014.
- Carey, Peter
Data Protection. A Practical Guide to UK and EU Law. 5th edition. Oxford University Press, 2018.
- Craig, Paul
de Búrca, Gráinne
EU Law. Text, Cases and Materials. 6th edition. Oxford University Press, 2015.
- Gutwirth, Serge
Privacy and the Information Age. 1st edition. Rowman & Littlefield Publishers, 2002.
- Lokke, Moerel
Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers. 1st edition. Oxford University Press, 2012.
- Schartum, Dag Wiese
Bygrave, Lee
Personvern i informasjonssamfunnet – en innføring i vern av personopplysninger. 1st edition. Fagbokforlaget Vigmostad & Bjørke, 2004.
- Van Alsenoy, Brendan
Regulating data protection: The allocation of responsibility and risk among actors involved in personal data processing. KU Leuven Faculty of Law, 2016. https://lirias.kuleuven.be/bitstream/123456789/545027/1/PhD_thesis_Van_Alsenoy_Brendan_archived.pdf Last accessed 09/04/2018.
- Voigt, Paul
Von dem Bussche, Axel
The EU general data protection Regulation – a practical guide. 1st edition. Springer International Publishing, 2017.

Articles

- Arrebola, Carlos
Mauricio, Julia
Portilla, Hector
Jimenez
An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union (2016). *Legal Studies Research Paper Series*. Paper 3/2016. University of Cambridge Faculty of Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2714259 Last accessed 08/03/2018.
- Blanc, Nicolas
Wirtschaftsakademie Schleswig-Holstein: Towards a Joint Responsibility of Facebook Fan Page Administrators for Infringements to European Data Protection Law? (2018). *European Data Protection Law Review*. Volume 4, Issue 1, p. 120-126. <https://edpl.lexxion.eu/article/edpl/2018/1/19> Last accessed 05/04/2018.
- Blume, Peter
Controller and processor: is there a risk of confusion? (2013). *International Data Privacy Law*. Volume 3, Issue 2, p. 140-145. <https://doi.org/10.1093/idpl/ipt002> Last accessed 22/03/2018.
- Blume, Peter
An alternative model for data protection law: changing the roles of controller and processor. *International Data Privacy Law*. Volume 5, no. 4, p. 292-297. https://www.researchgate.net/publication/282426276_An_alternative_model_for_data_protection_law_changing_the_roles_of_controller_and_processor Last accessed 04/02/2018.
- De Hert, Paul
Papakonstantinou, Vagelis
The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals (2012). *Computer Law & Security Review*. Volume 28, Issue 2. <https://doi.org/10.1016/j.clsr.2012.01.011> Last accessed 23/03/2018.
- Hogan Lovells
A Guide to Blockchain and Data Protection (2017). Link Last accessed 11/04/2018.
- Olsen, Thomas
Personvernøkende identitetsforvaltning (2015). *CompLex* 2/2015. http://www.complexserien.net/sites/complexserien/files/CompLex_2-15_web.pdf Last accessed 15/03/2018.

- Olsen, Thomas
Mahler Tobias Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust' (2007). *Computer Law & Security Report*. Part II, Vol. 23, No. 5, p. 415-426. <https://ssrn.com/abstract=1015006> Last accessed 12/03/2018.
- Sandtrø, Jan Databehandlers behandling av personopplysninger (2016). *Tidsskrift for forretningsjus*. Volume 22 no. 2-3, p. 69-151. https://www.idunn.no/tidsskrift_for_forretningsjus/2016/02-03/databehandlers_behandling_av_personopplysninger Last accessed 20/03/2018.
- Taylor Wessing *Data controller requirements under GDPR* (2017). <https://www.taylorwessing.com/globaldatahub/article-data-controller-requirements-under-gdpr.html> Last accessed 20/03/2018.
- Treacy, Bridget Challenging times ahead for data processors (2012). *Privacy and Data Protection*. Volume 12, issue 7, p. 3-6. https://www.hunton.com/images/content/3/5/v2/3523/Challenging_times_ahead_for_data_processors_Treacy.pdf Last accessed 27/03/2018.
- Van Alsenoy, Brendan
Ballet, Joris
Kuczerawy, Aleksandra
et al. Social networks and web 2.0: are users also bound by data protection Regulations? (2010). *Springer Netherlands. Identity Journal Limited*, 2009. <https://doi.org/10.1016/j.telpol.2015.07.014> Last accessed 20/03/2018.
- Van Eecke, Patrick
Truyens, Maarten Privacy and social networks (2010). *Computer Law & Security Review*. Volume 26, issue 5, p. 535-546. <https://doi.org/10.1016/j.clsr.2010.07.006> Last accessed 11/04/2018.
- Wolf, Christopher Impact of the CJEU's Right to Be Forgotten - Decision on Search Engines and Other Service Providers in Europe (2014). *Maastricht Journal of European and Comparative Law*. Volume 21, issue 3, p. 547-554. <http://journals.sagepub.com/doi/pdf/10.1177/1023263X1402100308> Last accessed 04/02/2018.

Others

- Deloitte About Deloitte. <https://www2.deloitte.com/global/en/pages/about-deloitte/articles/about-deloitte.html> Last accessed 24/04/2018.
- The Economist (2009) The Economist (2009). *Franchising*. <https://www.economist.com/node/14298990> Last accessed 12/03/2018.
- French, Carl *Data Processing and Information Technology*. 10th edition. Cengage Learning EMEA, 1996. <https://books.google.no/books?id=zVCdg7Tg6-AC&printsec=frontcover&hl=no#v=onepage&q&f=false> Last accessed: 02/03/2018.
- Hogan Lovells (2009) Lexology (2009). *Belgian data protection authority closes proceedings against SWIFT*. <https://www.lexology.com/library/detail.aspx?g=8c4f3e3e-9791-47d4-a049-26f6323eb9b5> Last accessed 23/04/2018.
- InterContinental Hotels Group Subscribe. <https://www.ihgplc.com/en/subscriptions/subscribe> Last accessed 24/04/2018.
- InterContinental Hotels Group Privacy Statement. https://www.ihg.com/content/gb/en/customer-care/privacy_statement Last accessed 24/04/2018.
- Obar, Joannathan Wildman, Steve (2015) Telecommunications Policy (2015). *Social media definition and the governance challenge: An introduction to the special issue*. Vol. 39, Issue 9. p. 745-750. <https://doi.org/10.1016/j.telpol.2015.07.014> Last accessed 19/03/2018.
- Oxford Dictionaries (2018) Authority. <https://en.oxforddictionaries.com/definition/authority> Last accessed 11/04/2018.
- Oxford Dictionaries (2018) Manipulation. <https://en.oxforddictionaries.com/definition/manipulation> Last accessed 11/04/2018.
- Rich, L. J. (2011) BBC News (2011). How can social networks make money? http://news.bbc.co.uk/2/hi/programmes/click_online/9457946.stm Last accessed 19/03/2018.