The GDPR’s lawful basis of legitimate interest
Advice and review regarding the balancing operation as of GDPR Article 6.1 (f)

Author: Dan Eriksson
Supervisor: Professor Carl Fredrik Bergström
Preface

Thank you to mom and dad for being great parents. I love you sincerely.

Professor Carl Fredrik Bergström deserves a ‘thank you’ as well, as he left valuable and candid comments while writing this thesis.

Would also like to thank a lot of other persons but since I respect their right to protection of their personal data and forgot to ask, I will not. (Professor Bergström’s name is already on the front page)…

Dan Eriksson,

Oslo, 29-03-2019
# Table of contents

## 1 Introduction

1.1 Background of this thesis ................................................................................. 8

1.2 Objectives of this thesis ..................................................................................... 9

1.3 Legal method and disposition ........................................................................ 9
    1.3.1 Legal method .......................................................................................... 9
    1.3.2 Disposition ............................................................................................. 10

## 2 General Data Protection Regulation

2.1 The relation to Primary EU Law ..................................................................... 11

2.2 GDPR and related laws .................................................................................... 13

2.3 GDPR’s main purpose and scope .................................................................... 15

2.4 Definitions ....................................................................................................... 17
    2.4.1 Personal data ........................................................................................ 17
    2.4.2 Processing ............................................................................................. 19
    2.4.3 Controller ............................................................................................. 20

2.5 WP 29 and the European Data Privacy Board: .............................................. 21

2.6 Principle of proportionality ............................................................................. 22

## 3 Data Protection Principles

3.1 The principle of lawfulness, fairness (and transparency) in conjunction with
    the principle of purpose limitation ..................................................................... 25
    3.1.1 Transparency criterion ......................................................................... 27
    3.1.2 Transparency and fairness ..................................................................... 29

3.2 The principles on storage, accuracy and collection ....................................... 29

3.3 The principle of integrity and confidentiality ................................................... 30

3.4 The controller’s accountability ........................................................................ 30
1 Introduction

In this introduction I would like to give light to the fact that personal data processing do affect people’s everyday life. If we take internet usage as an example, everybody has an opinion about different matters in life or society, but are you willing to state that opinion when it may be remembered forever, by whoever? Without having any statistical proof, I am willing to state that people are cautious to state their views online without the protection of at least believed anonymity. The thought of “this statement, even if made in confidence in a private conversation or by using a pseudonym - may be used against me later on in life” may create self-censorship\(^1\) that has not been present in earlier generations lives.

Use of small computers like smartphones, digital watches or smart-TV’s is extremely common in modern day life. And when looking at it with critical eyes and looking back in human history – this should become problematic if not handled responsibly.

The daily use of mentioned gadgets may be unproblematic at this point in time, but when reflecting more extensively about the amount of data that is collected and how this kind of data can be misused it is easy and reasonable to get a bad feeling in the stomach. As the world turns and regimes changes, it could become a nightmare. The fiction ‘1984’ by George Orwell could prove a point on a surveillance-society gone authoritarian, but the surveillance gadgets in Orwell’s novel is already in place. A big difference from the novel is that the current gadgets is on an even more sophisticated level technology-wise and that they have been added to our homes and pockets for the mere convenience they offer – not because they were imposed upon us by an oppressionist government as in the novel.

\(^1\) Colonna, Legal implications of data mining, page 208.
As times changes and regimes fall, all the collected data could and probably will be misused. In a time where deleting or anonymising information have become costlier than storing it\(^2\), stricter regulations are natural to aid the fundamental human right to protection of personal data and the related fundamental human right to privacy.\(^3\)

According to author’s opinion, data protection law should not only be seen as a burden for already stretched company budgets. The field of data protection law should, at least for businesses built on handling personal data as a business model, be given the same or even higher ethical significance than other currently more discussed laws as for example environmental law. And now with the European Union’s (‘EU’or ‘Union’)\(^4\) General Data Protection Regulation\(^5\) (‘GDPR’) in force, there should be economic incitement involved in addition to the ethical – as severe breaches of the GDPR may lead to extremely high fines.

Some major components in the GDPR except the rules on handling of personal data are the global scope of the regulation, the personal rights for registered individuals and the thorough accountability-scheme for responsible private actors. Worth mentioning is the extremely wide scope of the GDPR, that creates as strict legal obligations for companies that might not severely affect individuals’ privacy as for company which business model and profit is solely based on collection and thus, processing, of personal data.

For that reason, the GDPR enforcement created a lot of distress for companies that previously did not think about their business operations in a data protection law context. But since the GDPR is general in a strict sense, these businesses also need to comply with the regulation. The far-reaching scope created an epidemic of “consent requests” during the enforcement of the regulation. These requests were sent out when companies tried to comply with the rule on having at least one lawful basis for their handling of personal data. And related to this, I got the idea to aim this thesis on another lawful base

---

\(^2\) Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union".

\(^3\) The Charter Article 8 and 7.

\(^4\) In this thesis, I will use the term EU instead of EU/EEA.

for personal data processing: the lawful basis of “legitimate interest”, which in very short terms means that the party handling the personal data may have an interest of handling that is legitimate in comparison to the interests and fundamental rights and freedoms of the individual(s) whose data is concerned.

1.1 Background of this thesis

In the setting of the GDPR, when a personal data processing is carried out, the controller⁶ is responsible for compliance with the data protection principles.⁷ And to ensure that there is at least one lawful basis applicable for that processing.⁸ There are six different lawful bases in the GDPR, listed in Article 6.1 (a) to (f). They are in my opinion most easily described as:

(a) processing is based on the consent of the data subject.
(b) a contractual relationship requires the processing of personal data.
(c) processing is necessary for compliance with a legal obligation of the controller.
(d) vital interests of data subjects or of another person require the processing of their data.
(e) processing is needed for the performance of a task in the public interest.
(f) legitimate interests of controllers or third parties are the reason for the processing, but only as long as they are not overridden by the interests or the fundamental rights of the data subjects.⁹

As can be seen when comparing the lawful bases above, the legitimate interest (f) lawful basis does not have a specified setting for usage. It instead opens up for having an own interest as long as it is legitimate. However, it also adds an obligation to assess whether this interest will be overridden by the interests or the fundamental rights of the

---

⁶ Which means, the party determining the means and purposes of the processing, see GDPR Article 4 (7) for definition.
⁷ GDPR Article 5.2.
⁸ GDPR Article 6.
The balancing of the interests of the controller and the data subject(s) may require a complex assessment taking into account a number of factors.10

1.2 Objectives of this thesis

The objective of the thesis is to analyse law, case law, recommendations and opinions and to some extent legal doctrine to produce commercially viable advice (in other words, a check-list) on what to think about when conducting a balancing test according to the GDPR. I will finalise the thesis by a general discussion of some key points to the concept.

1.3 Legal method and disposition

1.3.1 Legal method

The methodology used when writing this thesis is a general legal method combined with the EU legal method. As the GDPR is a EU regulation, the interpretation need to be in line with the EU legal system. This is a fact since a EU regulation ideally should be given the same interpretation and enforcement in each and every member state. Therefore, case law from the Court of Justice of the European Union (‘CJEU’) will be the natural and correct choice of source when the GDPR needs to be clarified. And as there still is no for this thesis suitable case law produced for the GDPR, this thesis analysis of case law will be on the background of the former Directive11, and therefore sparse.

The main source except the regulation itself will be the recitals of the GDPR and former recommendations and opinions from Working Party 29 (‘WP 29’).

The thesis will be written in a manner that takes the legal hierarchy into observation. For example, before assessing a decision or opinion’s advice on a specific question – I will mention and compare with law or case law, if viable.

---

10 WP 217, page 23
11 Directive 95/46/EC.
Doctrine will be used to describe the core principles of data protection law and EU-law but will be scarcely used in the sections containing analysis, this demarcation is motivated by the fact that WP 29’s opinions are based upon the authorities that in fact enforces the regulation. This thesis will also scope in some parts of the EU primary law, including its legal principles and especially the Charter of Fundamental Rights of the European Union (The Charter) due to the fact that protection of personal data is a fundamental human right. As The Charter is inspired by the European Convention on Human Rights (ECHR), ECHR case law will be included as well.

1.3.2 Disposition
This thesis is dispositioned in a manner intended to give a background to the GDPR by firstly describing the regulation’s place in the EU legal system as a fundamental human right, then proceed into basic but relevant material provisions of the regulation. As the regulation is new while the fundamentals are old – a connection will be made to related laws and especially the replaced Directive.

This brief description of the GDPR’s purposes and place in the EU legal system will lead into the definitions relevant for answering this thesis main questions before proceeding into the provisions relating to the data protection principles – who creates an obligation to obtain at least one lawful basis for a processing of personal data.

This thesis will then proceed into describing the balancing operation called for when using the lawful basis of legitimate interest by referring to key points in the thesis descriptive parts. The summary is intended to be useful for a data controller when assessing if legitimate interest is a suitable lawful basis.

2 General Data Protection Regulation
This sections purpose is to firstly describe the GDPR in relation to its context in the EU legal system and then proceed into a brief history and description of the purposes of the legislation, once that is clear – I will describe key concepts of the regulation that is useful for understanding the following sections regarding the need for a lawful basis.
2.1 The relation to Primary EU Law

The primary EU law is the superior and the most basic level of the EU laws hierarchy of norms. The primary laws are often referred to as The Treaties, and The Treaties has changed and expanded continually during the lifetime of the now existent EU with the latest amendments made in 2016.12

The amendments to The Treaties often referred to as as the Treaty of Lisbon, year 2009, added the right to personal data protection in the Treaty on the Functioning of the European Union (TFEU) Article 1613. Furthermore, the amendments also made the EU Charter of Fundamental Rights (The Charter) legally binding by the Treaty of the European Union (TEU) Article 6.1, which states that The Charter shall have the same legal value as the Treaties.14

Going back to the GDPR, which is a secondary EU law and thus created with a basis in the primary EU laws:15 The legal basis for the GDPR is to be found in the preamble of the regulation which states: “Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof, […]”. This means that the GDPR’s founding primary law-article is TFEU Article 16.

When reading the recital 1 of the GDPR, references are made to The Charter as well as the TFEU. “Everyone has the right to the protection of personal data concerning [them]16 [him or her]17,”, this does not mean that the GDPR is based upon The Charter as well, but the recital pinpoints that the GDPR is aimed at protecting a fundamental human right within the EU legal system. And as The Charter has the same legal value as the Treaties, it needs to be taken into consideration when interpreting or exercising law within the EU’s given competences.18 In the subsequent paragraph, Article 8.2 of The

12 For all current Treaties in force, see: https://eur-lex.europa.eu/collection/EU_law/treaties/treaties-force.html
14 Note the TEU 6.1 second paragraph on the non-extension of any Union-competences, and The Charter Article 51.
15 Bergström & Hettne, Introduktion till EU-rätten, page 20. See also TFEU Article 288.
16 TFEU Article 16.1
17 The Charter Article 8.1
18 Bergström & Hettne, Introduktion till EU-rätten, page 25 and TEU Article 6.1 second paragraph.
Charter, it is stated that:

“Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”

This provision, stemming directly from The Charter, reinforce the importance of personal data processing to be fair, for a specific purpose, and based upon a lawful basis as consent – or another legitimate basis – laid down by law. I would also state that there is a direct need stemming from primary law to comply with the data protection principles (specified purposes) and the need for consent or another legitimate basis laid down by law (a lawful basis). The wording “right” in the provision shall however not be interpreted as an absolute right, but as a right that can be weighed against other rights.\(^\text{19}\)

It must also be noted in this primary law section that the GDPR confer to the right to protection of personal data and not the right to privacy\(^\text{20}\) (even if it often overlaps). In the ClientEarth case\(^\text{21}\), which were judged upon a regulation aimed to protect personal data within Community institutions\(^\text{22}\), the CJEU stated that the concepts of “personal data” and the “data relating to private life” were not to be confused.\(^\text{23}\) And that is a good point, since if only personal data that were “private” in its nature where seen as personal data, the scope of the data protection laws would be greatly narrowed.

A short note of the differences between personal data and private data and the need for protection of personal data in addition to protection of private data: a positioning-system of taxis is connected to the cars and not the drivers, but as there in fact is a driver driving that car – the positioning systems data will be personal data according to

\(^{19}\) See section 2.3.

\(^{20}\) The Charter Article 7.

\(^{21}\) Case C-615/13, Client-Earth.

\(^{22}\) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

\(^{23}\) Case C-615/13, Client-Earth, paragraph 32.
Working Party 29\textsuperscript{24} (WP 29).\textsuperscript{25} It would be harder to argue that the positioning system is private data as it relates to a car that (often) is owned by a company.

### 2.2 GDPR and related laws

Reconnecting to the above section regarding the difference between the right to protection of personal data as in The Charter’s Article 8, and the Article 7’s right to privacy. A lot of case law regarding personal data has been judged on the grounds of the right to privacy.\textsuperscript{26} The reason for this is that the right to privacy is closely related, and an older concept. For example, the UN recognise the right to private life\textsuperscript{27}, and the Council of Europe (CoE) protects the right to private and family life in the European Convention of Human Rights (ECHR).\textsuperscript{28}

Regarding the specific right to protection of personal data, The CoE founded the somewhat mother of modern data protection law with its 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which is commonly called ‘Convention 108’. The concepts from Convention 108 can be recognised when reading the data protection principles in the GDPR but also when comparing it to the wording from The Charter, as in previous section.\textsuperscript{29}

In Convention 108, Article 5:

**Quality of data**

*Personal data undergoing automatic processing shall be:*

*a. obtained and processed fairly and lawfully;*

*b. stored for specific and legitimate purposes and not used in a way incompatible with those purposes;*

*c. adequate, relevant and not excessive in relation to the purposes for which they are stored;*

\textsuperscript{24} See section 2.5 regarding WP 29.
\textsuperscript{25} WP 136, page 9. See the definition of personal data in section 2.4.1.
\textsuperscript{26} See ECHR, Guide on article 8, page 34 for a case law summary.
\textsuperscript{27} Article 12 of the United Nations Universal Declaration of Human Rights protects the right to private life.
\textsuperscript{28} See ECHR, Article 8.
\textsuperscript{29} See The Charter Article 8.2.
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

This means that the principles, but also a lot of rules, which the GDPR is based upon shall not be seen as a new, even if this was somewhat signalised in media during the enforcement of the regulation. The GDPR replaced the former Directive, which entered into force year 1995.

The Directive were similar to GDPR in many aspects and were aimed at the same goals as the GDPR, to protect the right to personal data. Without going into too wide of a discussion about if the GDPR is more important in a than the Directive: It is a fact that the GDPR imposes a lot stricter requirements on processing of personal data, especially since there are extremely high potential fines involved. But as GDPR is based upon the FEU(Article 16), which is incorporated into The Charter – the right to protection of personal data took a “step up” by the Lisbon Treaty as of 2009.  

This in my opinion gives the GDPR a bit more weight than the Directive seen from a hierarchy of norms perspective.

But the main purpose for the change from directive to regulation was not about the primary law. Instead, as directives in the EU legal system is only binding “as to the result to be achieved” and leaves a margin of appreciation to national authorities regarding the form and methods of implementation – the level of enforcement of the Directive varied in the EU member states. In recital 9 of the GDPR, these harmonization-problems are also mentioned as some of the purposes for the new legislation, since the inconsequence’s in application may hinder the pursuit of economic activities in the union, distort competition and impede authorities in the discharge of their responsibilities under EU law.

---

31 It could however be discussed if the Directive as of >2009 had the same or similar legal significance.
32 FEUF Art 288.
2.3 GDPR’s main purpose and scope

Reconnecting to above sections 2.1 and 2.2, the purpose of the GDPR is to strengthen natural persons rights regarding protection of personal data. In that sense, it is logical that the material scope is as wide as it is. This and the following sections will describe the material scope of the GDPR.

The wording “fundamental right” shall not be interpreted as an absolute right, but as a right that can be weighed against other non-absolute rights.\(^\text{34}\) That means that the GDPR is intended to protect individuals’ rights relating to personal data, but it may at the same time be out-weighted by other fundamental rights, as for example the right to conduct business\(^\text{35}\) or for the interests of the wider community.\(^\text{36}\) This applies to all the rights included in the GDPR as well, for example the commonly known ‘right to be forgotten’ as of GDPR Article 17.

In Joined Cases C-92/09 and C-93/09’s paragraph 50, the CJEU addressed The Charter’s Article 52.1, and stated that the right to personal data and privacy may be limited:

“[..]as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.”\(^\text{37}\)

The GDPR recital 2 states that:

“The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence,

\(^{34}\) Frydlinger & others, GDPR: - juridik, organisation och säkerhet enligt dataskyddsförordningen, page 30.

\(^{35}\) The Charter, Article 16

\(^{36}\) In joined cases C-92/09 and C-93/09, Advocate General Sharpston’s Opinion, ECLI:EU:C:2010:353, paragraph 73.

\(^{37}\) See also paragraph 48.49 of above advocate general’s opinion.
respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.”

As the GDPR is directed at “natural persons”\textsuperscript{38} and not EU citizens, the regulation also scopes in third country residents, which is a general trait in human rights legislations. For example, in The Charter, the rights are written in in-discriminatory terms like “everyone” and “no one” as: “Everyone has the right to life.”, and the sub-sequent Article 2.2 which states that “No one shall be condemned to the death penalty, or executed.”

This explains why the GDPR Article 3 regarding territorial scope is so widely formulated.\textsuperscript{39} In the Google Spain judgment\textsuperscript{40} where the territorial scope was examined, Google’s Spanish subsidiary claimed that the processing activities were carried out in the US and thus except from the former Directive’s applicability. The CJEU in its’ paragraph 52 and 53 came to the conclusion that (author’s underlining):

“51: Nevertheless, as the Spanish Government and the Commission in particular have pointed out, Article 4(1)(a) of Directive 95/46 does not require the processing of personal data in question to be carried out ‘by’ the establishment concerned itself, but only that it be carried out ‘in the context of the activities’ of the establishment.”

“53: Furthermore, in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively (see, by analogy, Case C-324/09 L’Oréal and Others EU:C:2011:474, paragraphs 62 and 63).”

The conclusion is that the scope is so widely formulated, since the regulation is intended to protect individuals’ fundamental rights and freedoms. Therefore the CJEU has

\textsuperscript{38} As in recital 2 mentioned above.
\textsuperscript{39} Except the obvious economic reasons of strengthening the internal market.
\textsuperscript{40} C-131/12, Google Spain.
applied an extensive interpretation of the former Directive’s scope, both materially and territorially. In the below section of 2.4 including sub-sections, the material scope of some key definitions will be analysed.

2.4 Definitions

As the following sections will use language from the GDPR, some of the definitions in the list of GDPR Article 4 will need to be described more thoroughly. Therefore, this section will describe the for this thesis relevant terminology of the GDPR and discuss the material scope of each definition.

Other terms that is useful for this thesis without going into more details is:

The data subject is the person who the personal data relates to. In other words, the individual.  

The data processor means the person (incl. legal persons) who in fact carries out the processing of the personal data.

2.4.1 Personal data

As the GDPR applies only to personal data, the first thing to assess when deciding if GDPR is applicable or not is whether the data is personal data.

GDPR Article 4(1):

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

I would say that the GDPR-definition is clear, but there has been produced a lot of case law regarding whether data is personal data or not. The reason for that should be that the replaced Directive were not as extensive. In comparison with above underlining, the

41 See GDPR Article 4 (1).
42 See GDPR Article 4 (8) and compare with section 2.4.3 Controller.
Directive used (from the word “in particular”): “by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”.

These changes to the definition are in line with case-law from the CJEU, which during the Directive judged that the following types of data are “personal data”:

ISP addresses (even dynamic), since they allow the user to be precisely identified, at least with support from the internet service provider. Fingerprint, as they objectively contain unique information about an individual which allows precise identification. Records of an employees’ hours of work, since they represent “information relating to an individual or identifiable natural person”. Images of a person, because it makes it possible to identify the person concerned. And also tax data regarding an individual.

This wide scope of the definition of “personal data”, should be connected to the purpose of the legislation, which is to ensure protection of personal data, not only “private” data.

But, since personal data can be both personal and private, it is feasible to expect that the personal data that fulfil both criterions should be regarded as somewhat ‘more’ personal data, as it will be protected by two basic human rights and not only one. This is supported by the extra rules regarding “processing of special categories of personal data” who are more private in their nature. In my opinion, this creates a situation where some data that is somewhat close to becoming “special category” may be regarded as a bit worthier of strict protection than the personal data furthest out in the spectrum.

---

43 C-70/10, Scarlet, paragraph 51.
44 C-291/12, Schwarz, paragraph 27.
45 C-342/12, Worten, paragraph 19.
46 C-212/12, Rynes, paragraph 22.
47 C-201/14, Bara, paragraph 29.
48 See section 2.3.
49 Also, ECHR Article 8, the right to respect for private and family life.
50 As in GDPR Article 9.
2.4.2 Processing

Article 4 (2) GDPR provides (author’s underlining)

“‘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;”

This means that in practice any handling of personal data is a “processing” of such. The GDPR definition gives 18 examples, but clearly states that other situations may be covered as well. Case-law from the CJEU provides an unsurprising hard approach and parties has not as often as with other definitions questioned if their handling of data is a “processing”. The CJEU has ruled that loading personal data on an internet page must be considered as a processing within the meaning of the old Directive.51 This should be clear from the wording in both the GDPR and the Directive, but what has been contested in for example below case law is to what extent this is reasonable.

In the Google Spain-case, Google argued that they are an indexing-service that only publish what has already been published, and that the original publisher is in fact carrying out the processing.52 This reasoning was rejected by the CJEU who interpreted the provision as it is written.53

Another example of several processing-activities taking place where in case Nikolau54 a leak to a journalist containing documents with personal data. When the company then made a press release about the leak and named the person – that was also considered a processing of personal data.55

---

51 C-131/12, Google Spain.
52 C-131/12, Google Spain, paragraph 26 with reference to Case C-101/01 Lindquist paragraph 25.
53 See also section 2.4.3 regarding the definition of controller’s last sentence.
54 T-259/03, Nikolaou.
55 T-259/03, Nikolaou, paragraph 204.
This is important as it clearly shows that each separate party or actor that in some way gets hold of the data, will be “processing” it. It shall be noted that the definition in GDPR is wider than that of the Directive, which could be related to the earlier caselaw produced regarding the scope of the definition.

2.4.3 Controller

The controller is the main responsible party for compliance with the GDPR, as for example the data protection principles\textsuperscript{56}, and by them, having at least one lawful basis.\textsuperscript{57}

GDPR Article 4 (7) states (author’s underlining): ‘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;

This provision points out, firstly, that the controller may be a natural or legal person. But also, the controller may be either a single person or several acting together as joint controllers.\textsuperscript{58} The determination of the means and purposes is the deciding factor on who obtains status as a controller in the GDPR. This means that the factual determination of means and purposes is the only thing that counts, and agreements stating otherwise will not be taken into account.\textsuperscript{59} In the Google Spain-case\textsuperscript{60}, the CJEU ruled that the search engine operator determines the purposes and means of the processing of personal data that it itself carries out within the framework of that activity,

\textsuperscript{56} GDPR Article 5.2.
\textsuperscript{57} GDPR Article 5.1 (a) and Article 6.1.
\textsuperscript{58} See GDPR Article 26 on joint controllers.
\textsuperscript{59} See also Frydlinger & others, GDPR: - juridik, organisation och säkerhet enligt dataskyddsförordningen, page 51.
\textsuperscript{60} C-131/12, Google Spain, paragraphs 32-41.
and consequently need to be regarded as a controller in respect of that specific processing.\textsuperscript{61}

The court added that: “Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of ‘controller’, effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.”\textsuperscript{62}

\subsection*{2.5 WP 29 and the European Data Privacy Board:}

The Article 288 of the TFEU regarding norms in the EU legal system provides:

"Recommendations and opinions shall have no binding force."

At the same time, this thesis and many books on data privacy law refers to WP 29, which created opinions and recommendations. This section describes why.

The WP 29 were a working group created during the Directive whose task were to interpret the EU data privacy law instruments and create guidelines and answer questions referred to them. The WP 29 consisted of one representative from each national data protection authority,\textsuperscript{63} a representative from the EU’s data privacy body and a representative from the EU commission.\textsuperscript{64} When the GDPR entered into force, the European Data Privacy Board (EDPB) replaced WP 29, who now have a corresponding function but with a more detailed task-list.\textsuperscript{65}

\textsuperscript{61} Compare with previous section, 2.4.2 mentioning case T-259/03, Nikolaou, which describes the separate processing activities.
\textsuperscript{62} C-131/12, Google Spain, paragraph 34.
\textsuperscript{63} Some countries, like Germany, have several data protection authorities, and picked one joint representative.
\textsuperscript{64} Directive Article 29, for DPB see GDPR Article 70.
\textsuperscript{65} Compare GDPR Article 70 and Directive Article 29.
As the EDPB act as the main organ among data protection authorities, the national data protection authorities will most probably regard the EDPB’s opinions and recommendations as something closely related to law\textsuperscript{66} – as they have with the WP 29’s.\textsuperscript{67}

And that is somewhat natural since the former WP 29 also was based upon the national data protection authorities’ employees, who seem to have agreed upon certain terms when interpreting the legislation. So even if recommendations and opinions have no legally binding force, the WP 29’s recommendations and opinions have greatly influenced and are still influencing how national data protection authorities and by them – also data controllers under their powers should act.

For that reason, the recommendations and opinions from the former WP 29 will be used as a source in this thesis regardless of their legally non-binding character. Worth noticing as well is that the EDPB on the day of GDPR entering into force (25\textsuperscript{th} May 2018), approved several of the WP 29 guidelines and opinions to be used for interpreting the GDPR.\textsuperscript{68}

In that sense, the WP 29 died and were replaced by the more powerful EDPB – but some of the recommendations and opinions lived on – and are now incorporated into a stronger and more powerful body.

\subsection*{2.6 Principle of proportionality}

The EU principle of proportionality is not a single principle but changes its character in different parts of EU law. It shall be noted that the concept is not originally from the EU, but a widespread general legal principle found in liberal democracies.\textsuperscript{69} One part of

\textsuperscript{66} Or what some people call “soft-law”.


\textsuperscript{68} The European Data Protection Board Endorsement 1/2018.

\textsuperscript{69} Tridimas, T, The General Principles of EU Law, page 136.
the principle that nowadays are codified in TEU is a norm aimed at the EU legislators when creating law and is referring to the EU principle of conferral. The “law-creating proportionality principle’s” goal is to avoid that the EU goes too far in their legislative process compared to the Treaties. 70

The principle of proportionality relevant for this thesis is related to the following section 6 regarding the balancing of interests. This means that when a legislation is enforced, the legislator (and if passed, the courts) shall make a proportionality assessment where the limitation of a human right is weighted against the legitimate goal it is intended to reach.

The principle of proportionality that is useful for this thesis is the “general” legal principle of proportionality. In EU law, as in other jurisdictions, the “general” principle of proportionality determines whether intervention by authorities or governmental bodies can be motivated by public interests. 71 Therefore, the principle of proportionality applies not only to courts but also authorities when exercising its powers in general.

A good example is case C-189/01 ‘Jippes’72, were a member state authority took unproportionate measures against an individual to comply with EU regulations by confiscating a lady’s pet sheep in order to comply with an EU regulation.73

Except the short insert above about the pet sheep Jippes, the case C-343/09 Afton Chemical, paragraph 4574 provides guidance on the principle (author’s underlining):

“According to settled case-law, it must be recalled that the principle of proportionality, which is one of the general principles of Community law, requires that measures adopted by Community institutions do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must

70 As in Treaty of the European Union Article 5, including the principle of subsidiarity.
72 C-189/01, Jippee’s.
74 Case C-343/09 Afton Chemical, paragraph 45 with references to other cases.
be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued[...]

For the purpose of describing the principle, below “principle of proportionality for dummies” could be used:

1. Suitability – is the measure suitable or relevant to realizing the goal it is aimed at meeting?
2. Necessity – is the measure required for realizing the goals it is aimed at meeting?
3. Non-excessiveness – does the measure go further than necessary to realise the goals it is aimed at meeting?  

The principle of proportionality per se is not included in the data protection law principles, though it underpins the principles of data protection legislation and may analogically be used when assessing if a personal data processing is legitimate or not.  

This is manifest in for example the quoted judgment of joined cases C-92/09 and C-93/09, Volker und Markus Schecke and Hartmut Eifert, paragraph 48-50 regarding the balancing of fundamental human rights.

3 Data Protection Principles

This sections aim is to provide an overview of the GDPR data protection principles as in GDPR Article 5.1 (a) to (f), for which the controller shall be able to demonstrate compliance with. The for this thesis most relevant data protection principles are given separate sub-sections including references to the obligation of having a lawful basis

76 Bygrave, L-A, Data Privacy Law, page 148.
77 Paragraph 50 quoted in section 2.3, see also Advocate General Sharpston’s Opinion, ECLI:EU:C:2010:353, paragraph 73.
78 GDPR Article 5.2.
while the data protection principles that is out of scope of this thesis is given a very brief description.

To give some extra weight to the data protection principles it shall be stated that all the rights and obligations of the GDPR can be said to in one way or another give reason to or aim to fulfil the data protection principles.\textsuperscript{79} Adding to that, the main data protection principle of “lawful and fair” form part of the EU primary law.\textsuperscript{80}

Seen from the commercial sector, the data protection principles shall be seen as important liability-wise as a controller’s\textsuperscript{81} non-compliance with the data protection principles is included in the category of non-compliance that may lead to the maximum level of fines (up to € 200 000, or 4\% of total worldwide annual turnover, whichever is greater), as in GDPR Article 83.5.\textsuperscript{82}

\textbf{3.1 The principle of lawfulness, fairness (and transparency) in conjunction with the principle of purpose limitation.}

GDPR Article 5.1 (a), personal data shall be:
“processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);”

Fair and lawful has been the main theme since Convention 108 and is part of the written EU primary law.\textsuperscript{83} For the part of the principle relating to transparency, see sub-section 3.1.1 and 3.1.2.

\textsuperscript{79} Frydlinger & others, GDPR: - juridik, organisation och säkerhet enligt dataskyddsförordningen, page 34.
\textsuperscript{80} See section 2.1 on GDPR’s relation to EU primary law.
\textsuperscript{81} See section 2.4.3.
\textsuperscript{82} Compare with GDPR Article 83.4.
\textsuperscript{83} See section 2.1.
The twin-criteria of “fair and lawful” can be said to be the primary principle of data protection law as these twin criteria’s is manifest in all other data protection principles. The lawfulness-criteria stems from the fact that protection of personal data is a fundamental right, and all such rights shall be governed by law. The fairness criteria means that data controllers must take into account the interests and reasonable expectations of the data subjects. The principle of fair and lawful processing, and especially the part of fair referring to the reasonable expectations of the data subject is interconnected with the principle of purpose limitation as in GDPR Article 5.1 (b) which states that personal data shall be:

“collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);”

Partly, the principle is grounded on concern for ensuring foreseeability for data subjects when their personal data is processed. Practically it means that when a processing of personal data is conducted for a specific purpose, this purpose may not change to fit a new purpose without informing the data subject of the new purpose for the processing-operation. A change of purpose may only be done with a clear legal basis.

84 Bygrave, L-A, Data Privacy Law, page 146. See also the corresponding wording in The Charter’s Article 8.2 and Convention 108’s Article 5.
85 See section 2.6 on the principle of proportionality.
86 Bygrave, L-A, Data Privacy Law, page 146, see also Wp217 page 40, point iv)
87 WP 217, page 40, point iv).
In a case from the ECHR where Sweden was up against a data subject, the court addressed the purpose limitation principle of the Convention 108’s Article 5.2, see author’s underlining to pinpoint the sentence relating to “reasonable expectations”90: Although the records remained confidential, they had been disclosed to another public authority and therefore to a wider circle of public servants […] Moreover, whilst the information had been collected and stored at the clinic in connection with medical treatment, its subsequent communication had served a different purpose, namely to enable the Office to examine her compensation claim. It did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office.91

3.1.1 Transparency criterion

The criteria of GDPR Article 5.1 (a) regarding “in a transparent manner” means that the data subject shall be aware of the processing taking place and receive edible information about the extent of the processing activity.92 The criteria of ‘transparency’ is not defined in the GDPR, but GDPR recital 39 is informative as to the meaning and effect of the principle.93 GDPR recital 39 provides that:

“All processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect

90 Inter-thesis reference to my description of the fairness-criteria in GDPR Article 5.1 (a)
91 (1999) 28 EHRR 313, case MS vs Sweden
93 WP 260 “Guidelines on transparency under Regulation 2016/679”.

27
of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.\[\ldots\]

The criterion of transparency may also be seen in for example GDPR Article 7 on consent, that states in its second paragraph (author’s underlining):

*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

Another example of the “in a transparent manner” is the entire section 1 of the GDPR, which contain extensive requirements on transparency when either collecting or receiving personal data.\(^94\) This is supplemented by a data subject right, the “right of access by the data subject”\(^95\), which simplified can be described as a directly enforceable right to know if a data controller processes a data subjects individual personal data.

The criterium of transparency is mentioned in several GDPR-provisions, and the most obvious example is the right to transparency in GDPR Article 12, which connect to the right to gain insight in the data processing, and the informing of data subjects that personal data processing is taking place. Comparing with the Directive’s Article 6 (b), the addition of the transparency criteria is the main difference, whereas it can be said that this was baked into other provisions of the Directive, the GDPR makes it a clear basic principle and governs it with administrative fines. This will in my opinion believably lead to a stricter enforcement of the principle in upcoming judgments than during the Directives days, as it since GDPR enforcement is a possibility to use the principle seen on its own for claims against the data controller.

---

\(^{94}\) As in GDPR Article 13 and 14.

\(^{95}\) See GDPR Article 15
3.1.2 **Transparency and fairness**

GDPR Article 12\(^\text{96}\) contain the main rules on giving transparent information to data subjects whose data is or will be processed. The rules provide that the communication shall be “concise and transparent”, which means that the data controller shall present the information efficiently and succinctly in order to avoid information fatigue.\(^\text{97}\) It also provides that the information shall be “intelligible” which means that it should be understood by an average member of the intended audience.\(^\text{98}\) In other words, the information should be tailored to fit their group of data subjects.\(^\text{99}\) A central consideration of the principle of transparency is that the data subject at hand shall be able to foresee the scope and consequences of the personal data processing that will take place.\(^\text{100}\) In other words: There shall be no unpleasant surprises.\(^\text{101}\)

For that reason, the transparency-criteria is highly relevant when assessing whether a processing is fair and lawful, and by that – it also gives purpose when balancing interests between the controller and the data subject as of this thesis main subject – the lawful basis of legitimate interest.

### 3.2 The principles on storage, accuracy and collection

The data protection principles of GDPR Article 5.1 (c) to (e) relates to storage, accuracy and the scope of collection of personal data. As this thesis relates to the lawful bases, these principles will only be mentioned in short. The principle of data minimisation\(^\text{102}\) can in my opinion most easily be described as a rule on continually reviewing if the stored, collected or otherwise processed personal data are as minimalistic as possible. The principle of accuracy relates to keeping personal data accurate and where necessary

\(^{96}\) See also GDPR Articles 13-14 (information to data subjects), GDPR Articles 15-22 (exercising individual rights) and GDPR Article 34 (communication of data breaches).

\(^{97}\) WP 260, page 8.

\(^{98}\) See also WP 217, page 31 on what a reasonable person would expect.

\(^{99}\) WP 260, page 8.

\(^{100}\) WP 260, page 7.

\(^{101}\) Everybody likes pleasant surprises!

\(^{102}\) GDPR Article 5.1 (c)
The principle of accuracy is in my opinion not that hard to comprehend, as inaccurate personal data is hard to make purposeful, necessary, or compatible with any of the other principles. The principle of storage limitation means that once the processing of personal data is un-necessary for the purposes for which they are processed – they shall be deleted. The principle of storage limitation is effective once data is stored – while the principle of data minimisation is more of a general demand to not collect excessive personal data.

### 3.3 The principle of integrity and confidentiality

as of GDPR Article 5.1 (f) states that personal data shall be:

“processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

In short, this principle state that appropriate technical and organisational measures need to be taken to protect personal data. This could for example be to have proper policies and procedures in place, an IT-system that is appropriate for the risks involved for data subjects, or standardised anonymisation of personal data once into the hands of the controller. By using the GDPR recital 83 to interpret this provision, the requisite of appropriate depends on the economic strength of a company and the risks involved for data subjects. For that reason, various levels of measures could be regarded as “good enough” for this principle.

### 3.4 The controller’s accountability

GDPR Article 5.2 states: “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”

---

103 GDPR Article 5.1 (d)
104 GDPR Article 5.1 (e)
This creates an obligation to acquire clear allocation of responsibilities between controller(s) and processor(s) when carrying out processing operations.\textsuperscript{105} This obligation is generally remedied by data processing agreements\textsuperscript{106} between the parties, which in some cases creates a contractual problem when neither party want to acquire the compliance obligations by being classified as a controller.

This is a misconception of the regulation. And I would say that many companies and individuals see it as “ownership” of the personal data. However, the GDPR does not use the term “data owner”.\textsuperscript{107} And this should create an interest to comply with the data protection, as it can be hard to determine whether a party is acting as a controller or a processor, and the party that in fact determines the means and purposes of a specific processing operation is accountable for that operation, and thus, compliance with the data protection principles.\textsuperscript{108}

It is hard to put words to what is fair, and the general view of what fairness connotes will change over time. It is also hard to pronounce what fair means in a EU law context, as the GDPR applies on a EU level and, while the member states citizens undoubtedly will have different views on what fair collection of data means – depending on their trust in society on a general level but also relating to how digitalised the country at hand is. History of certain parts of Europe should also make the application of a general view of fair very hard, as states who were authoritarian in the 1990’s most probably will have a less relaxed feeling about registries and collection of information than for example Scandinavia. This should mean that the CJEU’s views on what connotes fairness might be stricter than expected in Scandinavia.

\textsuperscript{105} GDPR Recital 79
\textsuperscript{106} GDPR Article 26
\textsuperscript{107} See section 4.1.3 regarding the definition of controllership
\textsuperscript{108} GDPR Article 26.10
4 Lawful basis

Any personal data processing shall comply with the above-mentioned data protection principles\(^{109}\), and be processed lawfully, fairly and in a transparent manner – this implies that the processing must be not illegitimate and have a lawful basis.\(^{110}\)

There are six different lawful bases according to GDPR Article 6 and at least one must always apply. For special categories of personal data (often called sensitive personal data), there is additional requirements and restrictions as of GDPR Article 9.

As of GDPR Article 6:\(^{111}\)

The first basis, (a), is when the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

The second basis, (b), is when processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

The third basis, (c), is when the controller needs to process the personal data in order to comply with its’ legal obligations.

The fourth basis, (d), is when the processing of personal data is necessary in order to protect the vital interests of the data subject or of another natural person.

The fifth basis, (e), is when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The sixth, (f), and maybe the most used lawful basis in the private sector except consent-requests is the legitimate interest purpose. When this lawful basis is used, it must be assessed whether the legitimate interests pursued by the controller or by a third

---

\(^{109}\) As of GDPR Article 5.
\(^{111}\) List inspired of Handbook on European Data Protection Law, 2018, page 141ff
party are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This does not apply to governmental bodies, authorities or similar who shall act according to law or instructions otherwise accepted in the member states.

As will be shown in the following sections, picking a suitable lawful basis (or bases) is a hard task.

4.1 Consent

In this subsection I have made a short notion about the concept of consent – simply because it is the most discussed lawful basis of the GDPR and was used a lot\(^\text{112}\) during the months leading up to enforcement of the GDPR. A good example on the back-side of using consent (for the controller) is provided by WP 29 in its opinion 15/2011 ‘on the definition of consent’ where an ID-card functionality from a state authority is described (author’s underlining):

*New ID cards with electronic functionalities embedded in a chip are being developed in Member States. It may not be compulsory to activate the electronic services of the card. But without activation, the user could be prevented from accessing certain administrative services, which would otherwise become very difficult to reach (transfer of some services on-line, reduction of office opening hours). Consent cannot be claimed to be the legitimate ground to justify the processing. In this case the law organising the development of e-services, together with all the appropriate safeguards, should be the relevant ground.*\(^\text{113}\)

In above example, the ID cards is not compulsory, but it is not a totally free choice either since the consequences are negative if you do not consent. And therefore, the lawful basis of consent can not be used. Instead, the WP 29 referred to the lawful basis of authority vested in the controller. However, this does not mean that there is a general rule hindering the lawful basis of consent to be used as soon as there is a minor negative

\(^{112}\) Check your e-mail inbox for received e-mails during April and May 2018.

\(^{113}\) WP 189, page 16.
consequence. For example, if you do not consent to registering for a supermarket’s customer card and therefor do not receive rebates – that is your choice – and the controller (the supermarket) will have obtained a valid consent with the ones that in fact did consent.114

A (from a data controllers point of view) problematic part of the lawful basis of consent is that it can be withdrawn at any time.115 This means that sending out consent-requests could be a less commercially minded idea if there is a more rigid116 lawful basis to rely upon.

115 GDPR Article 7 (3).
116 As in easier to comply with.
5 Lawful basis of legitimate interest

The lawful basis of legitimate interest is the last listed ground allowing for lawful processing of personal data. It calls for a balancing of the interests of the controller (or third parties) against the fundamental rights and freedoms of the data subject. This ‘balancing operation’\textsuperscript{117} determines whether this lawful base may be relied upon as a legal ground for processing.

This section (5) will be structured as follows:

5.1 – Interpretation and summary of the GDPR-provisions,
5.2 – Case law relating to GDPR Article 6.1 (f),
5.3 – WP 29’s opinion on legitimate interest.

5.1 Interpretation and summary of the GDPR-provisions

The GDPR Article 6.1 (f) states that processing under this basis shall be lawful only if (author’s underlining):

“processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

And the following sentence states that:

“Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.”\textsuperscript{118}

The provision contains three main requirements which should be read in the light of GDPR recital 47. The three requirements: 1. Purposefulness for fulfilling the legitimate interest at hand; 2. A necessity criterion; and 3. The balancing of the controller(s)

\textsuperscript{117} WP 217, page 9.
\textsuperscript{118} A hint that authorities shall act according to written law, which includes the EU law. See for example The Administrative Procedure Act of Sweden, paragraph 5.
interest of data processing against the interests or fundamental rights and freedoms of
the data subject.\textsuperscript{119} It should be pointed out that both the controller(s) and the data
subject may have interests. But the provision pinpoints that the controller(s) interests
must be legitimate, while the data subject’s interest-criteria does not contain that
limitation.

5.1.1 \textbf{Recital 47}

In the following, I will split recital 47 up by using quotes and connect each split-up to
the written law. The first sentence of recital 47 provides:

\textit{The legitimate interests of a controller, including those of a controller to which the
personal data may be disclosed, or of a third party, may provide a legal basis for
processing, provided that the interests or the fundamental rights and freedoms of the
data subject are not overriding, taking into consideration the reasonable expectations
of data subjects based on their relationship with the controller.}

This is in my opinion a reference to the following GDPR\textsuperscript{120} data protection principles:
1. purpose limitation principle,\textsuperscript{121} and: 2. the “fairness” and “transparency” criteria’s in
the principle of lawful, fair and transparent processing.\textsuperscript{122}

The first part of recital 47 (according to author) refer to the possible processing
operation of transmitting\textsuperscript{123} personal data (as in the first part of the sentence: “the
legitimate interests of a controller, including those of a controller to which the personal
data may be disclosed”) to another controller. This means that if the processing takes
place for the purpose of making it available to another controller (often by a request) –
an assessment needs to be done (by the first controller) whether this second controller’s
interest is legitimate – in addition to its own interests. This creates a need to, in case of

\textsuperscript{119} The data subjects which concern all fundamental rights, but in this case it is directed towards the right
of protection of personal data and the right to privacy. See GDPR recital 1 and The Charter’s Article 8 and 7.
\textsuperscript{120} Widely applied in other data protection and privacy laws. See section 2.2.
\textsuperscript{121} See section 3.1 regarding the purpose limitation principle.
\textsuperscript{122} See section 3.1.1 and 3.1.2 on transparency.
\textsuperscript{123} Transmitting is a “processing”, see section 2.4.2.
transfers, get information from the “requesting” controller prior to making the information available.

This should mean that an interest of for example, “We have a legitimate interest to transmit the personal data for the purpose of avoiding that “other controller” cancel our current service agreement during the next renewal.”, is illegitimate, as the controller holding the personal data will need to assess whether the “other controller” have a legitimate interest once the personal data gets in its hands. Therefore, if the processing at hand involves transfers to third party controllers, the lawful basis of legitimate interest creates an obligation to assess the third-party controller’s legitimate interest – in addition to its own.

The second part of the first sentence of recital 47 states “taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.”, which should be a clear hint that especially fairness and transparency as in section 3.1 of this thesis need to be ensured when relying on the lawful basis of legitimate interest.

The second sentence of recital 47 states that:

Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

The data subject’s relationship with the controller could according to my assessment turn the table on above case regarding the purpose limitation principle, and the wording of this part of the recital may give some proof to it. The reasonable expectations of the data subject will have to be corresponding to the factual processing.124

The following wording of recital 47 provides accordingly (author’s underlining):

“At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The

124 See section 3.1.1 and 3.1.2 regarding transparency.
interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.”

“Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.”

This is a change from the Directive125, where public authorities were not explicitly forbidden to use the corresponding lawful basis of legitimate interest.126 And for that reason, interpretation of old case-law regarding the lawful basis of legitimate interest should be done with care, at least when looking at personal data processing carried out by public authorities.

“The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.”

These two sentences of the recital 47 gives two practical examples, which is a bit strange since there are loads of situations were examples would be needed. If it is strictly necessary, fraud-prevention constitute a legitimate interest. However, processing of personal data for direct marketing is mentioned as well – but not given any “green” or “yellow” light from the legislator. Therefore, I guess the direct marketing-part of the recital were added after some rounds of lobbying in Brussels, and for that reason, processing for direct marketing using this lawful basis should be given no more legal significance than other possible legitimate interests. Instead, it should be seen as an example of a possible legitimate interest. This example will in my opinion most likely create hassle as companies will base their processing on legitimate interest and just refer

125 The last sentence in GDPR Article 6.1, which states “Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.”
126 See above comment in 5.1 regarding EU and member states administrative laws.
to recital 47 without carrying out the balancing of interests and fundamental rights and freedoms.

5.2 Case law relating to GDPR Article 6.1 (f)

The case law referred to in this section where judged on the legal grounds of the Directive, where the lawful basis of legitimate interest as of Article 7 (f). The old case law on this subject does not provide that much guidance that is not already included into GDPR, but in my opinion there is two cases worth mentioning:

In Case C-13/16 (Riga Case), the CJEU used a three-step method to evaluate the legitimate interest, which in my opinion is the only logical way of testing the legitimate interest as there is three main requisites.

In the Riga Case, a data subject had opened a taxi door and damaged a public transport vehicle. The owner of the transport vehicle wanted to obtain personal data from the police authority in order to bring actions for damages in a civil court. The main question to the CJEU was if the data controller, the Latvian police authority, had an obligation to disclose personal data to a third party that had been damaged by the data subject. The question at hand is not that relevant for this thesis, and there was no legal obligation in the Directive and neither there is in the GDPR. But, the question lead to a situation where the legal basis of legitimate interest was somewhat addressed. According to author’s interpretation, the paragraphs 31 to 33 of the Riga Case provides that (author’s wording):

When balancing the opposing rights and the other parties interests at hand, it depends on the specific circumstances of the particular case.

---

127 See also Directive Article 5, stating that the implementation into member states may vary, within the limits of Article 7’s lawful bases.
128 C-13/16, Riga.
Considerations can be taken to the possibility of accessing the personal data in public sources. So, in other words, if the data can be accessible by a search on Google or by contacting an authority, the infringement in the data subject’s fundamental right to protection of personal data is not that much of an infringement as if it were more secret data.\(^{130}\)

The CJEU states that one of the factors which should be taken into account when balancing the interests is the age of the data subject.\(^{131}\)

By this statement, the CJEU opens up for other factors that could be taken into account, which however is pretty obvious.

In the point 32, the CJEU referred to the joined cases of C-468/10 and C-469/10 where the CJEU in its 44\(^{th}\) paragraph stated:

“In relation to the balancing which is necessary pursuant to Article 7(f) of Directive 95/46, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject’s fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources.”

I would say that this is the main point from CJEU case law regarding the lawful basis of legitimate interest. The view should in my opinion depend on which member states that is at hand, since some national jurisdictions keep public registers very public according to their constitutional law. If this were interpreted extensively, although it would be against the essence of the GDPR, for example Swedish citizens would become less protected from the GDPR due to its strong legal tradition of public access\(^{132}\) – compared

---

\(^{130}\) C-468/10 and C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito, paragraph 44.

\(^{131}\) It was a minor that caused the damages. See GDPR recital 38 regarding children’s extra protection regarding consent.

\(^{132}\) See the Public Access to Information and Secrecy Act and the constitutional Press Act’s section 2, paragraph 1.
to other national jurisdictions within the Union. In other words, this CJEU judgment shall be seen in the context of the GDPR, and therefore be interpreted restrictively.\textsuperscript{133}

5.3 WP 29 opinion

In ‘Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC’\textsuperscript{134}, the WP 29 parties produced their views on the lawful basis of legitimate interest. I will summarize the in my opinion relevant advices and comment them in a free manner.

WP 29 states regarding the concept of “interest” (author’s underlining):

“\textit{The concept of 'interest' is closely related to, but distinct from, the concept of 'purpose' mentioned in Article 6 of the Directive. In data protection discourse, 'purpose' is the specific reason why the data are processed: the aim or intention of the data processing. An interest, on the other hand, is the broader stake that a controller may have in the processing, or the benefit that the controller derives - or that society might derive - from the processing.”}\textsuperscript{135}

This means that an interest is the “goal”, and the purpose is the way to reach to the goal. For example, a purpose can be to implement a system that will fulfil the interest. An interest must furthermore according to WP 29 be sufficiently clearly articulated to allow the balancing test to be carried out against the fundamental rights and interests of the data subject whose personal data may be processed.\textsuperscript{136}

\textit{“In the view of the Working Party, the notion of legitimate interest could include a broad range of interests, whether trivial or very compelling, straightforward or more controversial. It will then be in a second step, when it comes to balancing these interests against the interests and fundamental rights of the data subjects, that a more restricted approach and more substantive analysis should be taken.”}

\textsuperscript{133} See section 2.
\textsuperscript{134} WP 217.
\textsuperscript{135} WP 217, page 24.
\textsuperscript{136} A a s.
So this means that it is possible to have a trivial interest and a controversial purpose at first. And then the next step will be to see if it may be justified. The view of the WP 29 is that even if the balancing test shows that the data subject’s right shall prevail and thus stop or not conducting the processing, the appropriate safeguards\textsuperscript{137} may justify the processing.\textsuperscript{138}

5.3.1 Assessing the controller’s legitimate interest

WP 29 states that it is impossible to make value judgments with regard to all possible legitimate interests, but it is possible to provide some guidance. The WP 29 then proceeds into mentioning that the fundamental rights and freedoms contain a lot of different elements that may come into conflict with the right to protection of personal data. These could be freedom of expression, right to access to documents, freedom to conduct business – and so on. When these norms collide, the processing shall be proportionate and necessary.\textsuperscript{139}

For the private sector, WP 29 notes that (author’s underlining):\textsuperscript{140}

\textit{It can also be the case that a private business interest of a company coincides with a public interest to some degree. This may happen, for example, with regard to combatting financial fraud or other fraudulent use of services.\textsuperscript{81} A service provider may have a legitimate business interest in ensuring that its customers will not misuse the service (or will not be able to obtain services without payment), while at the same time, the customers of the company, taxpayers, and the public at large also have a legitimate interest in ensuring that fraudulent activities are discouraged and detected when they occur.}

And this should be considered when conducting the first part of the balancing test. The wider the beneficial sphere is, the more proportionate a measure will be. And it goes back to the general principle of proportionality which states that a measure shall be “necessary and proportionate measure in a democratic society”\textsuperscript{141}, furthermore the WP 29 adds that:\textsuperscript{142}

\textsuperscript{137} For example, encryption, strict security or similar.
\textsuperscript{138} WP 217, page 34.
\textsuperscript{139} WP 217, page 34, see also this thesis section 2.6 regarding proportionality.
\textsuperscript{140} WP 217, page 36.
\textsuperscript{141} See section about the principle of proportionality.
\textsuperscript{142} WP 217, page 36.
“The more explicitly recognised it is in the law, in other regulatory instruments - be they binding or not on the controller - or even in the culture of the given community overall without any specific legal basis, that the controllers may take action and process data in pursuit of a particular interest, the more heavily this legitimate interest weighs in the balance.”

According to author, the legal principle of proportionality is here referred to. As all laws within the EU’s member states shall have been trialled or at least interpreted according to the principle of proportionality143 – these laws can be used for assessing whether an interest is legitimate or not, regardless of their applicability in the specific case.144

5.3.2 The impact on the data subjects

WP 29 states that several elements can be useful when assessing the data processing’s impact on data subjects. These include: the nature of the personal data, the way the information is processed, the reasonable expectations of the data subjects and the status between the controller and data subject.145

“In assessing the impact of the processing, both positive and negative consequences should be taken into account. These may include potential future decisions or actions by third parties, and situations where the processing may lead to the exclusion of, or discrimination against, individuals, defamation, or more broadly, situations where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject.

In addition to adverse outcomes that can be specifically foreseen, broader emotional impacts also need to be taken into account, such as the irritation, fear and distress that may result from a data subject losing control over personal information, or realising that it has been or may be misused or compromised, – for example through exposure on the internet. The chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration.”146

In above quote with author’s underlining, WP 29 mentions that extensive processing may lead to self-restriction that harms for example the freedom of speech. In my

143 See section 2.6 regarding the principle of proportionality.
144 If they were applicable, the lawful basis of legal obligation as in GDPR Article 6.1 (c) would have been the correct lawful basis.
145 WP 217, page 36.
146 WP 217, page 37.
opinion, this leads to the conclusion that when interpreting GDPR, the risk based analysis of the consequences for a data subject must be wider than in most areas of law, and thus – the causal chain when assessing negative impact need to be wider than in most areas of law.

WP 29 states it as “It is also important to understand that more often than not a series of related and unrelated occurrences can lead cumulatively to the ultimate negative impact on the data subject and it may be difficult to identify which processing activity by which controller played a key role in the negative impact.” 147

According to me, this reconnects to the first sentence of GDPR recital 47 which imposes an obligation upon the controller to assess not only its own legitimate interest but also the legitimate interest of another controller that will gain access to the personal data. 148

As WP 29 points out clearly in this sentence, which I think is the best final words on the impact assessment (author’s underlining):

The Working Party emphasises that it is crucial to understand that relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of the data processing. For the sake of clarity, we also emphasise that the concept is unrelated to the notion of data breach and is much broader than impacts that may result from a data breach. Instead, the notion of impact, as used here, encompasses the various ways in which an individual may be affected - positively or negatively - by the processing of his or her personal data. 149

In other words, putting up a pro’s and con’s list with possible consequences and benefits should be a good idea to start the balancing test. This list should be extensive to include possible consequences that the data controller is not directly responsible for. It goes in line with the legal obligation to ensure sufficient guarantees that the processor implements appropriate technical and organisational measures before they carry out processing of personal data on behalf of a data controller. 150

147 WP 217, page 37.
148 See my comment regarding purpose limitation in section 5.1.1.
149 WP 217, page 37.
150 GDPR Article 28.1.
a processor that does not even know about its’ legal obligations, but signs an agreement stating that they do is a good example of the beginning of a malign causal chain.

5.3.3 Provisional balance

WP 29 stated that “When balancing the interests and rights at stake as described above, the measures taken by the controller to comply with its general obligations under the Directive, including in terms of proportionality and transparency, will greatly contribute to ensuring that the data controller meets the requirements of Article 7(f).”

In other words, this reference to the transparency-principle points out that the data subject’s informational situation regarding the processing is a key factor when conducting the balancing test. In my opinion, this creates a stricter requirement on informing the data subject when using the lawful basis of legitimate interest compared to some other lawful bases. The purpose for this is that the lawful basis of legitimate interest shall not become an opening that renders the whole lawful basis-article meaningless.

Furthermore, WP 29 advises (author’s underlining): “Additional measures may include, for example, providing an easily workable and accessible mechanism to ensure an unconditional possibility for data subjects to opt-out of the processing. These additional measures may in some (but not all) cases help tip the balance and help ensure that the processing can be based on Article 7(f), while at the same time, also protecting the rights and interests of the data subjects.”

So, when conducting the balancing test, it is possible to come to the conclusion that the processing is not suitable, but when taking measures to protect the data subjects at hand – it may become legitimate. Such measures could be opt-out options as the WP 29 suggest, but I guess it could also be to for example add contractual protection stating that any external sub-processors will not be used, or similar. See next section.

---

151 WP 217, page 41
152 A a s.
153 A a s.
5.3.4 Additional safeguards applied by controller to prevent any undue impact on the data subjects

As shortly described above, the balancing of the interest may be affected by applying appropriate measures to protect the data subject at hand. Whether then these measures will make the processing legitimate will depend on the assessment of all relevant circumstances.\(^{154}\) WP 29 states that adding additional information about the processing (in excess of the legal obligation) is one way to come forth. Other ways may be:\(^{155}\)

- “technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals (‘functional separation’ as is often the case in a research context)
- extensive use of anonymisation techniques
- aggregation of data
- privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments
- increased transparency
- general and unconditional right to opt-out
- data portability & related measures to empower data subjects”

Above measures may all, according to WP 29, in a positive way tip the scale to the conclusion that a processing of personal data is legitimate under the lawful basis of legitimate interest.

5.4 Author’s opinion

Following in my own foot-steps of trying to describe provisions according to the legal hierarchy, I have placed my own opinion below WP 29’s opinion. In section 2.6 the general principle of proportionality was described. I would not state that the principle of proportionality is directly applicable to the test when determining if a data controller’s processing is necessary to fulfil the purposes of the legitimate interest – however, as any

\(^{154}\) C-13/16, Riga, paragraph 31.
\(^{155}\) WP 217, page 42.
authority exercising EU law is bound by the principle, it is reasonable to use it when working with requisites as “necessary”, “[not] excessive”, “fairness”, “appropriate” and similar. The earlier scheme described to easily test the principle of proportionality in EU law:¹⁵⁶

1. Suitability – is the measure suitable or relevant to realizing the goal it is aimed at meeting?
2. Necessity – is the measure required for realizing the goals it is aimed at meeting?
3. Non-excessiveness – does the measure go further than necessary to realize the goals it is aimed at meeting?¹⁵⁷

According to author, a way of assessing necessary is to look at the goal of the processing, look at the chosen way to reach this goal – and then assess whether there is another way forward with the same result achieved but with less intrusion of privacy. Such measures could be to put contractual obligations on a processor prior to entering into a service agreement, for example to ensure that there is no general authorisation to use sub-processors without a written approval.

6 Balancing of the interests as of GDPR Article 6.1 (f)

When a controller has decided to use the lawful basis of legitimate interest as a ground for processing personal data – the balancing operation needs to be conducted. This section is aimed at the commercial sector, and references are made to my reasoning by references to sections within this thesis. The subsequent discussion in section 7 will discuss key points in a more academic manner.

A key to conduct a balancing test is to have a clear purpose of the intended processing of personal data and a conclusion that there is a need to process the personal data. The

¹⁵⁶ Referred to as the general principle of proportionality for dummies, furthest to the rear in named section.
purpose may be important or not important, but if there is a way of reaching this purpose without processing the data. The following advice will be meaningless. But as long as there is a need, there may be a way.

An indicator that the controller’s purpose is legitimate can be:
1. The controller wants to exercise a fundamental right itself.158
2. A similar processing is allowed by law for a similar purpose, regardless of the law’s applicability in this specific processing.159

When assessing the amount of possible impact on the data subjects, and thus balancing the interests, questions asked can be:
1. What kind of personal data is involved?160 Is the personal data publicly available?161
2. Will other controllers receive the personal data?162 If so be the case, are their purposes for receiving the personal data legitimate? Will the personal data become public because of the processing?163
3. What are the reasonable expectations of the data subject, taking into consideration the relationship between controller and processor?164
4. Are we (as in “controller conducting the analysis”) transparent regarding the processing?165
5. What is the worst-case scenario?166
6. What can be done that will increase security for the personal data, and thus minimise

---

158 See section 2.3 regarding GDPR as a non-absolute right, including caselaw regarding The Charter Article 52.1.
159 See last quote of section 5.3.1.
160 See section 2.4.1 with my discussion about data that is both private data and personal data.
161 See section 5.1 regarding publicly available personal data, and section 5.2 regarding Riga Case.
162 See section 5.1.1 on my interpretation of the criteria of “including those of a controller to which the personal data may be disclosed”.
163 This applies by argumentum a contrario from the Riga Case, where public available data is seen as less worthy of protection. See section 5.2 for CJEU statement.
164 See sections 3.1.1 and 3.1.2 on data protection principle of transparency.
165 A a s.
166 See section 5.3.2 regarding impact on the data subjects and my comment regarding extensive causal chains.
the risks involved?167

7. If the processing involves sending or transmitting the personal data: Is the processing governed by accountability, in other words, is the further processing foreseeable?168

167 See section 5.3.4 on additional safeguards according to WP 29 and section 3.3 regarding the obligation to implement technical and organisational measures.

168 See section 3.4 regarding accountability, especially regarding processing agreements.
7 Last words

As the GDPR’s purpose is to protect individuals right to protection of personal data by having a general law that then may be deviated from, instead of having specific provisions forbidding certain processing operations of personal data – the EU created a set of rules that is almost impossible to comply with.

In such a setting, it is important to bear in mind that the purpose of the legislation has been partly fulfilled. By creating a law that almost no normal company will understand, and almost no company will have the resources to buy understanding for, the EU obtained its objective and created massive deletions of personal data within companies, and migrated servers back to Europe.

With that said, I will go back to the lawful basis of legitimate interest:

When having a first look at the lawful basis of legitimate interest without knowing the law in general, it is easy to see it as an easy way out of the hassle with for example consents. But as could be read in this thesis, the concept is complex and incorporates a lot of basic legal knowledge, as for example the principle of proportionality and weighing of fundamental rights in The Charter. It also adheres to a fully stuffed law that in total is 88 pages long (including recitals) named the GDPR.

My advice for a data controller that thinks about using the lawful basis of legitimate interest is to only use it as a substitute for the other lawful bases in cases where there is an easy answer to my two above lists with questions.

I dearly hope that the authorities of EU will come to some kind of edible conclusions regarding concepts like this and provide easily available solutions to the ones who are paying the largest part of their budget: The companies and by them, their employees that have to manage the legislations unclear provisions in their daily work.
8 Bibliography

Literature

Colonna, L, Legal Implications of Data Mining, 2016.


Opinions and recommendations

Working Party 29:

WP 217 “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”.


WP 260 “Guidelines on transparency under Regulation 2016/679”.

WP 187 “Opinion 15/2011 on the definition of consent”.

Other


Webpages

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union":

Case law

Case C-615/13, Client-Earth and PAN Europe.

C-131/12, Google Spain.

Joined cases C-92/09 and C-93/09, Volker und Markus Schecke and Hartmut Eifert, and: Advocate General Sharpston’s Opinion, ECLI:EU:C:2010:353.

Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito.

C-101/01, Lindquist.

C-275/06, Promusicae.

C-342/12, Worten.

C-212/12, Rynes.

C-201/14, Bara.

C-291/12, Schwarz.
C-70/10, Scarlet.

T-259/03, Nikolaou.

C-189/01, Jippee’s.

C-13/16, Riga.