LUND UNIVERSITY

SCHOOL OF ECONOMICS AND MANAGEMENT

Direct Marketing in light of GDPR

When processing of personal data is lawful for conducting direct marketing, from a Swedish perspective

Ludwig Nikolai Trana

DEPARTMENT OF BUSINESS LAW

Master Thesis in European and International Trade Law

15 credits

HARN63

Spring 2024

Contents

Abstract

The thesis deals with which legal basis seems appropriate to use when the purpose of the data controller is to carry out direct marketing. When processing personal data, the Controller must comply with the principles set out in Article 5 of the GDPR. One of the principles, the Principe of Lawfulness, requires the Processing to be supported on a legal basis in Article 6 of the GDPR. It is stated that three of the six legal bases in Article 6 (1) GDPR can apply to such processing of personal data. The thesis consists of a presentation of the legal basis of the performance of a contract, as well as legitimate interest and consent. It should be noted that it is not appropriate to support a treatment for the exercise of direct marketing on the performance of a contract. To support such a Processing on the performance of a contract, it is required that the processing is necessary for the performance of the contract, which is rather difficult to demonstrate.

Legitimate interest is an appropriate legal basis for those who wish to engage in direct marketing. The controller must conduct a balancing of interests to examine whether the data subject's legitimate interest outweighs the data subject's interest and fundamental rights and freedoms. In most cases, balancing interest should result in the controller being allowed to exercise such processing for direct marketing purposes. To avoid a balancing of interests and a requirement that the processing must be necessary, the Controller may choose to base its processing on consent, which may justify even a so-called unnecessary processing.

Keywords: Marketing, Direct Marketing, GDPR, Lawfulness, Legal basis, Consent, Legitimate Interest.

Abbreviations

Article 29-working Party	A Working Party, set up under Article 29 of directive 95/46/EC. It was an independent European advisory body on data protection.
CJEU	Court of Justice of the European Union
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
E-privacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
EU	European Union
EU-charter	EU Charter of Fundamental Rights
FEDMA	Federation of European Data and Marketing
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
HFD	Swedish Supreme Administrative Court
Prop.	Government bill
ICC	International Chamber of Commerce
IMY	Swedish Supervisory Authority
MFL	The Swedish law regarding marketing.
SOU	Swedish Government Official Reports
TFEU	Treaty of Function of the European Union

1 Introduction

1.1 Background

Marketing is essential for companies in terms of new customer contacts and maintaining existing customer contacts. Through marketing, businesses can increase their sales, strengthen their brand, and improve their market position in relation to competitors. In today's digital society, we face a large amount of marketing expressed in different ways and forums. According to an article from Red Crow Marketing, people encounter between 4,000 and 10,000 ads daily.[1] Even before the person leaves their home in the morning, it is estimated that they have observed around 500 advertisements. According to an interview survey conducted on behalf of the Swedish Consumer Agency in 2013, 84% of the consumers surveyed answered that they had been subject to telemarketing in the past year, which is also a form of marketing.[2]

There are different types of marketing communication, including "ordinary" advertising in newspapers or television, advertising on social media with or without profiling of the target group, direct marketing, which takes place, for example, through e-mail, and personal sales, such as telemarketing. Depending on the type of marketing communication a company chooses to use, it may face different legal challenges. Legislation on personal data, marketing, and the right to purchase are examples of areas of law that may be relevant for the company to consider.

When it comes to direct marketing, there is a particular need for the processing of personal data as this type of marketing communication means that the direct marketer targets the marketing to specific individuals. In this context, there is a need to establish an understanding of the terminology, which is why an explanation of the definitions follows below.

The International Chamber of Commerce (ICC) defines direct marketing in its Advertising and Marketing Communication Code of 2018, which clarifies its meaning.

> "is the communication, by whatever means, of advertising or marketing material carried out by a direct marketer itself or on its behalf, and which is directed to particular individuals using their personal contact information (including mailing address, telephone number, email address, mobile phone number, facsimile, personal social media account handle, and the like)."[3]

A similar definition of direct marketing can also be found in the Federation of European Data and Marketing (FEDMA) Code of Conduct on the use of personal

[1] See Marshall, Ron. How Many Ads Do You See In One Day? *Red Crow Marketing INC.* 2015-09-10. <https://www.redcrowmarketing.com/blog/many-ads-see-one-day/> (Accessed 2024-05-20)

[2] See SOU 2015:61. *Ett stärkt konsumentskydd vid telefonförsäljning*, page 30.

[3] See International Chamber of Commerce (ICC), ICC:s Advertising and Marketing Communication Code, 2018, page 30.

data for direct marketing. Furthermore, the Code of Conduct also reproduces a definition for Direct marketer:

> "Any natural or legal person, including charities and political parties) who communicates by whatever means (including but not limited to mail, fax, telephone, on-line services etc,…) any advertising or marketing material which is directed to particular individuals."[4]

The definitions of direct marketing and direct marketer suggest that marketing communication takes place directly between the marketer and the individual who participates in the marketing.[5] When the marketer targets marketing directly to an individual, the processing of their personal data, such as phone number, email address, or username on social media, is required, which means that the marketer has to comply with the General Data Protection Regulation 2016/679 (GDPR)[6].

An important question for those who wish to engage in direct marketing is: What legal basis can the processing of personal data be based on? Of course, an assessment should also be made based on what personal data can be processed, how long the processing can be carried out, and what information will be provided to the individual. A complex question arises when deciding which legal basis allows the processing to be considered lawful in accordance with the GDPR. Factors such as the type of personal data, the direct marketer's ability to obtain consent, and the security measures taken should play a decisive role in the choice of legal basis. Thus, this thesis will investigate which legal basis may be appropriate when exercising direct marketing.

1.2 Purpose and Research Questions

The purpose of this thesis is to describe and analyse the legal basis on which personal data processing can be based when the controller conducts direct marketing to comply with the principle of lawfulness.

The purpose of this thesis will be answered on the basis of the following questions:

I. When can Article 6 (1) (b) of the GDPR (performance of a contract) be used as a legal basis for processing of personal data when conducting direct marketing?

II. When can Article 6 (1) (f) of the GDPR (legitimate interest) be used as a legal basis for processing of personal data when conducting direct marketing?

III. When can Article 6 (1) (a) of the GDPR (consent of the data subject) be used as a legal basis for processing of personal data when conducting direct marketing?

---

[4] See Federation of European Direct and Interactive Marketing (FEDMA), European Code of Practice for the Use of Personal Data in Direct Marketing Electronic Communications Annex, Brussels. 2010, page 3.

[5] Compare advertising in newspapers aimed at the public.

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

1.3 Delimitations

The thesis will exclusively deal with legal bases which can be used in direct marketing when the controller is not a public body. The demarcation is the consequence of the limitation of space. As a result of the delimitation, the legal basis of public interest will not be the subject of investigation in this thesis. Furthermore, it follows from the purpose of the thesis, personal data processing for the purpose of direct marketing, that the legal basis of fundamental interest is not relevant and is therefore not the subject of investigation in this thesis. Finally, the legal basis of legal obligation will not be dealt with in this thesis because there is no such legal obligation to conduct direct marketing toward data subjects. Since the starting point is the legal basis, an account of the basic principles is required, which is done sparingly.

1.4 Method and Materials

In the presentation of the thesis, an EU law method has mainly been applied in combination with a traditional legal method, also called a legal dogmatic method. The relationship between the EU law and the legal dogmatic method is rather complex. Identifying a legal issue based on EU law requires the EU law method, which should appear natural. The legal dogmatic method should be understood as a general method for dealing with legal issues, at least as far as Sweden is concerned, whereby the EU law method constitutes a supplementary method due to the distinctive character of EU law.

As a student with a Swedish legal education, I find it natural to relate to the legal dogmatic method, especially with regard to the doctrine of sources of law. By applying the legal dogmatic method, the answers to a legal question are sought in the accepted sources of law. The procedure can be described in such a way that the legal problem is to be solved, in which case the answers are sought in the text of the law, case law, preparatory work, and legal literature.[7] The starting point for the presentation of the thesis is thus to interpret current law, *de lege lata*, in order to answer the prescribed question.[8] It is of great importance that the legal situation is presented through a fair presentation, which is why I have observed an objective approach while at the same time achieving transparency through careful reference management, as a result of the requirement for scientific acreage.[9]

Throughout the thesis, the doctrine of sources of law is taken into account and respected, taking into account the legal dignity of the sources of law, both regarding Swedish law and EU law. Regarding the Swedish sources of law, the starting point

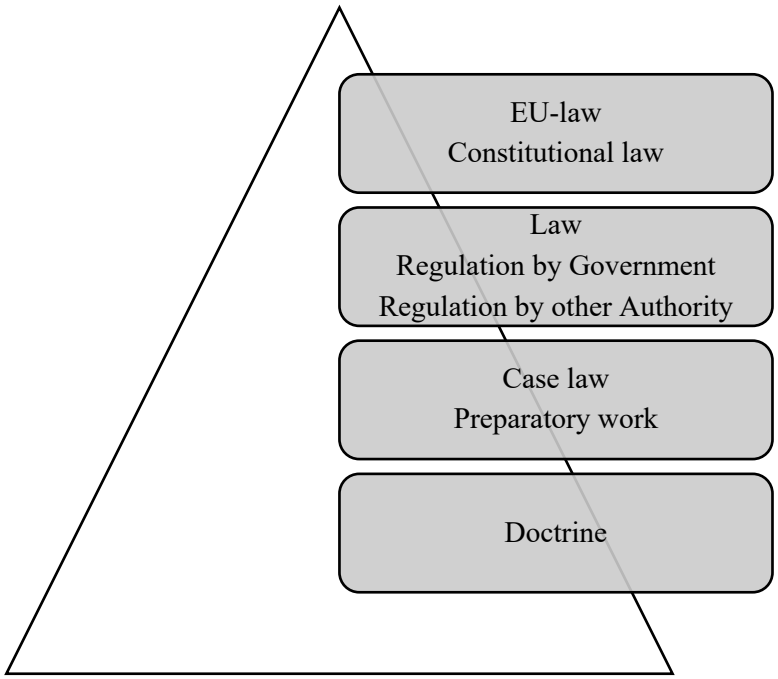
[7] See Kleinemann, Jan. Rättsdogmatisk Metod. *Juridisk Metodlära*. Nääv, Maria and Zamboni, Mauro (red.). 21 – 46. 2th ed,. Lund: Studentlitteratur, 2021. [Cit: Juridisk Metodlära] page 21.

[8] See Juridisk Metodlära, page 25.

[9] Ibid., pages 36 – 38.

has been the current constitution, which possesses high legal dignity, as only the Swedish constitution and EU law (with some reservations) are given precedence.[10]

As a result of the general wording used in the drafting of the law, it is far from sufficient to seek answers from this source of law. Of these, Swedish preparatory work and case law have also been the subject of investigation. Statements in the preparatory work express the legislator's intended application of the law and thus contribute to an understanding of how the text of the law should be interpreted. However, the preparatory work should not be regarded as binding. As far as case law is concerned, this demonstrates that the law is applied in practice in which a court has interpreted the law. The starting point for using case law is precedent decisions from the Supreme Administrative Court. Still, I find it relevant to describe decisions from administrative courts of appeal since such decisions can contribute to essential reasoning. A significant source of law for me is the doctrine, which, on the one hand, has low legal dignity but, on the other hand, is a source that gives a more detailed account and contributes to a deeper analysis of the legal situation. While the court is bound to interpret current law, authors of the doctrine are not bound and can thus carry on discussions that extend beyond current law.[11]



NORM HIERARCHY IN SWEDISH LAW[12]

As a result of Sweden's accession to the European Union (EU) in 1995[13], Swedish law and the Swedish sources of law came to be affected by EU law. Such an impact also entailed a need to apply the EU law method, as EU law can be described as

[10] See Bernitz, Ulf, Carlosson, Mia, Heuman, Lars, Leijonhufvud, Madeleine, Magnusson Sjöberg, Cecilia, Seipel, Peter, Warnling Conradson, Wiweka and Vogel, Hans-Heinrich. *Finna rätt, - Juristens källmaterial och* arbetsmetoder. 15th ed., Stockholm: Norstedts Juridik 2020. [Cit: Finna rätt] pages 30 – 31.

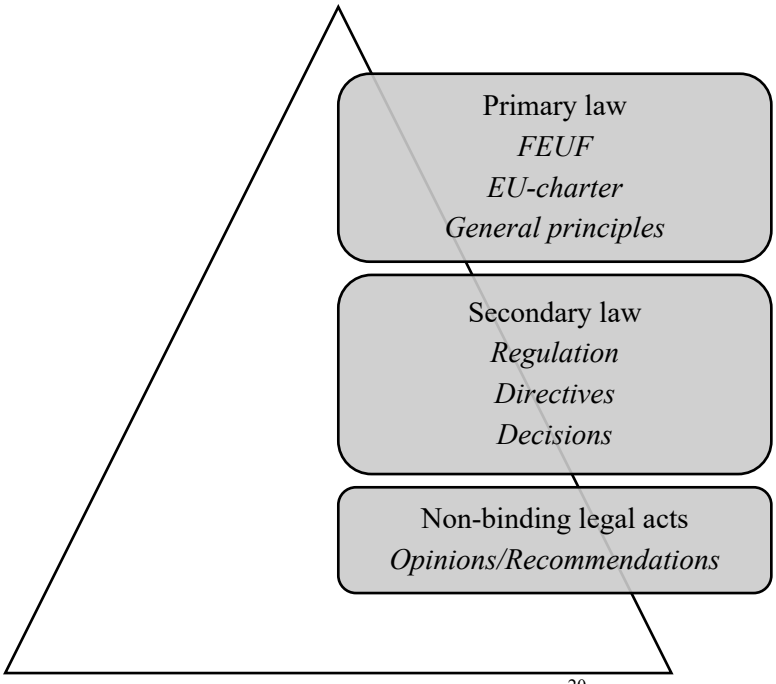
[11] Ibid. page 32, where they highlight the importance of doctrine in the legal system.

[12] Simplified illustration of the Swedish norm hierarchy with inspiration from Finna rätt.

[13] See European Comission. Sweden and the Swedish membership. <https://sweden.representation.ec.europa.eu/om-oss/sverige-och-eu-medlemskapet_sv> (Accessed 2024-05-01)

unique.[14] EU law has a strong focus on the rights of the individual, which created "private enforcement" whereby the individual can assert his or her rights under EU law in national courts.[15] Two essential differences between national law and EU law are, on the one hand, the hierarchy of norms of EU law and, on the other hand, how the Court of Justice of the European Union (CJEU)interprets it.[16] EU law consists of a comprehensive set of rules of law in which general principles of law play a significant role without being codified in primary law.[17] In the EU legal system, there are three main divisions of regulatory frameworks: primary law, secondary law, and soft law. In secondary legislation, a distinction is made between regulations, directives, and decisions. After its adoption, a regulation is directly applicable as the law in force in all Member States without prior implementation.[18] Directives, on the other hand, must be implemented by national law to apply as applicable law, except for direct effect provisions.[19]

When interpreting a legal act from the EU, such as the GDPR, a relatively strong purpose-oriented interpretation must be made, a so-called teleological interpretation. Prominent in the doctrine of interpretation of EU law is the systematic interpretation, which means that the provision that is the subject of interpretation must be interpreted in the context in which it is located. The teleological interpretation means that the provision is interpreted in the light of its purpose, which, in my view, is the leading method of interpretation in EU law.



HIERARCHY OF NORMS IN EU LAW[20]

[14] See Hettne, Jörgen and Otken Eriksson, Ida (red.). *EU-rättslig metod – Teori och genomslag i svensk rättstillämpning.* 2th ed., Stockholm: Norstedts Juridik, 2011. [Cit: EU-rättslig metod] page. 34.

[15] Ibid. page 21.

[16] Ibid., pages 36 – 37.

[17] See Finna rätt, page 63.

[18] See EU-rättslig metod, pages 177 – 178.

[19] Ibid. pages 178 – 185.

[20] Simplified illustration of the hierarchy of norms in EU law with inspiration from Finna rätt, page 63.

As a result of the prescribed question, the starting point for the thesis has been GDPR. To establish a deeper understanding of the provisions of the GDPR, its preamble has helped deduce the purpose of the provisions. I have used case law from both Swedish courts and the CJEU, which has provided guidance on how different courts have chosen to interpret the provisions. As I determined, the case law presented in the thesis constitutes a selection of available case law. Furthermore, I have used both case law, which deals with provisions in the GDPR, while a large part of the case law relates to Directive 95/46/EC, which remains relevant in line with the CJEU's statement.[21] I find it very valuable to use the doctrine, national and international, combined with the opinions and recommendations of the European Data Protection Board (EDPB) (formerly the Article 29 Working Party). The choice to use the opinion of the Article 29 Working Party is based on a selection of opinions that I do not find obsolete and which still today have a source of law.

1.5 Outline

In the second chapter of the thesis, a background to the GDPR is presented together with an explanation of its applicability and essential concepts. In this chapter, it also sets out the basic principles that must be complied with when processing personal data.

Chapter three consists of an account of the legal basis for the performance of a contract, in which the legal prerequisites for its application are discussed.

Chapter four deals with the legal basis of legitimate interest, the legal prerequisites for this together with guidance in the exercise of a balancing of interests.

The fifth chapter deals with the legal basis of consent together with a presentation of special situations in which case there is a requirement for consent.

Finally, the thesis is summarised in chapter six.

[21] See Judgement of 7 Mars 2024 in Case C-604/22, *IAB Europe,* ECLI:EU:C:2024:214, paragraph. 33 with reference to Judgement of 17 June 2021 in Case C-597/19, *Mircom International Content Management & Consulting (M.I.C.M) Limited v Telenet BVBA.* ECLI:EU:C:2021:492, paragraph.107.

2 Data protection law

2.1 Applicable Legislation

As a preliminary point, it is necessary to recall the background of data protection law, which is needed to understand its applicability. Most of the acts of high legal standing provide for a right to privacy for the individual. The first time the right to privacy was enshrined in a legal document was through the European Convention on Human Rights (ECHR) in 1950. Article 8(1) of the ECHR provides that individuals have the right to privacy and the protection of their correspondence. The ECHR has been ratified by all EU Member States, and 47 states have ratified the Convention. Ratification is such that the ratified State undertakes to respect the rights guaranteed by the Convention. Following the adoption of the Treaty of Lisbon in 2009, the EU has the legal possibility of ratifying the ECHR, which it has not yet done.

The CJEU has stated in Opinion 2/13 plenary that ratification by the EU is incompatible with Article 6 TEU.[22] In that regard, it should be noted that the CJEU has stated that fundamental rights are a general principle of EU law.[23] In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108.[24] Convention 108 was the first international legal document in the field of data protection.

Since its adoption in 1958, Article 16 TFEU has provided for a right to the protection of personal data in the EU. Since then, EU citizens have been guaranteed the right to privacy and respect for their private, family, and communications by Articles 3 and 7 of the EU Charter, which was adopted in 2000 and has had the status of a treaty since the adoption of the Treaty of Lisbon in 2009.

To ensure EU citizens their fundamental rights and freedoms, including the right to protection of their personal data (privacy), as explained above, the Data Protection Directive 95/46/EG was adopted in 1995 and subsequently replaced by the current Regulation 2016/679 (GDPR). The legislator chose to adopt regulation and thus replace the directive to ensure a uniform application of data protection within the EU. The Commission's evaluation of the implementation of the Data Protection Directive did not find this satisfactory due to a difference in application for different Member States.[25]

I do not find any reason to question the need for regulation in the area of data protection, but I believe that such a need is both strong and clear. In order to ensure

[22] See Opinion of 18 December 2014 in Case Opinion 2/13, *Opinion pursuant to Article 218(11) TFEU,* ECLI:EU:C:2014:2454, paragraph. 37.

[23] See Opinion 2/13, *Opinion pursuant to Article 218(11) TFEU,* paragraph. 37.

[24] See WP 179. 0836-02/10/EN. *Opinion 8/2010 on applicable law.* Adopted 2010-12-16, page 7.

[25] See WP 217. 884/14/EN. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* Adopted 2014-04-09, page 8.

the protection of privacy on the part of the EU and effective cooperation between the Member States, it is a disturbing factor if the legislation, even if to a very small extent, differs from one Member State to another. That was the case in ASNEF and FECEMD[26], which alleged the incorrect application and transposition of the Data Protection Directive by a Member State.

Joined Cases C-468/10 and C-468/10

In the present case, the Court has stated that the purpose of the Directive is to ensure an equivalent level of protection in all Member States. In that case, the Court had to interpret the Member State's transposition of Article 7.[27] The list set out in that article was exhaustive, and the Member State, therefore, had no possibility of either extending or restricting that list.[28] It is important to note that the Court has pointed out that the article has a direct effect.[29]

2.2 Introduction to GDPR

2.2.1 The Purpose of GDPR – Article 1 (1)

On April 27, 2016, the GDPR was adopted and became applicable two years after its adoption. It should be recalled at the outset that the GDPR has been set out in the prescribed objectives, which are two in number. The objectives can be deduced from the heading and Article 1 (1) of the GDPR. The GDPR aims to protect natural persons when their personal data is subject to processing.[30] Consequently, it is apparent from Article 1 (2) of the GDPR that the fundamental rights and freedoms of natural persons, in particular the protection of personal data, are guaranteed. The second purpose stipulates that the GDPR should promote the free flow of personal data. A regulation and thus the "same" rules for the processing of personal data within the Union promote processing in the internal market as the personal data is subject to the same protection regardless of the Member State in which the processing takes place. The GDPR also includes the possibility of transferring personal data to a third country, a so-called third-country transfer, through, for example, an adequacy decision for a third country (a country without the EU). Thus, we can see provisions promoting personal data's free flow. In order to meet the requirements of free movement within the Union, it is therefore essential that personal data can also be transferred between different Member States; if this were not the case, the movement of capital, persons, goods, and services would have been significantly impeded.

[26] See Judgement of 24 November 2011 in Joined Cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado.* ECLI:EU:C:2011:777.

[27] See Article 6 in GDPR.

[28] See Joined Cases C-468/10 and C-468/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado.* paragraphs 29 – 30.

[29] Ibid. paragraph 55.

[30] See C-604/22, *IAB Europe* paragraph. 53, with reference to Judgement of 15 July 2021 in Case C-60/20, *Latvijas dzelzels VAS v Valsts dzelzcela administracija.* ECLI:EU:2021:610, paragraph. 64.

2.2.2 Material and Territorial Scope – Articles 2 and 3

The GDPR becomes applicable partly based on material conditions according to Article 2 of the GDPR and partly through the fulfilment of the territorial conditions stipulated in Article 3 of the GDPR. The GDPR applies to the processing of personal data that is wholly or partly carried out by automated means and to processing that is not carried out by automated means but where the personal data is or will be included in a register. In this context, personal data is understood as any information relating to an identified or identifiable natural person. An identifiable natural person is a person who can be identified directly or indirectly.[31] The definition of personal data in the GDPR provides, non-exhaustively, examples of personal data such as name, location data, and financial information of the data subject.[32] It has since been expressed in case law that IP address and TC strings constitute personal data as defined.[33]

> An Internet Protocol (IP) address is an address through which it is possible to identify which device is interacting with the Internet. A TC (Transparency and Consent String) is a sequence of letters or characters that contains the preferences of the internet user as regards his or her consent to the processing of his or her personal data. A TC string is used to obtain consent to a kind of CMP (Consent Management Platform) through which the consent can be passed on to other suppliers so that they can, for example, send marketing to the person who has given their consent.[34]

Processing is defined as an operation or combination of actions concerning personal data, regardless of whether it is carried out by automated means or not.[35] The processing of personal data pursuant to Article 2 (1) GDPR is excluded from the scope of the GDPR, in which case the processing of personal data for private use is one of the exceptions.

Furthermore, the GDPR is applicable provided that the controller or processor has a place of business in the EU, regardless of whether the processing is carried out inside or outside the EU. However, as neither the processor nor the controller has an establishment within the Union, the GDPR may apply if the processing is carried out on personal data belonging to natural persons located in the Union insofar as the processing is related to the offering of goods and services to data subjects in the Union or where monitoring is carried out by natural persons in the Union. A third procedure that entails the GDPR becoming territorially applicable is when the processing of personal data is carried out by a controller outside the Union but in a place where a Member State's national law is applied, for example, at a Member State's embassy in a non-EU Member State.

---

[31] See Article 4 (1) GDPR. See Judgement of 19 October 2016 in Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland,* ECLI:EU:C:2016:779, paragraph.43, which provides that the information constitutes personal data where the data subject is identifiable by all means that can reasonably be used, even where the controller does not possess all these means alone. See also Judgement of 7 Mars 2024 in Case C-479/22, *OC v. Commission*, ECLI:EU:C:2024:215, paragraphs. 45, 48 and 55. WP 136. 01248/07/EN. *Opinion 4/2007 on the concept of personal data*. Adopted 2007-06-20, page 15.

[32] See Article. 4 (1) GDPR.

[33] See C-604/22, *IAB Europe*, paragraph. 45.

[34] Ibid., paragraphs. 24 – 26.

[35] See Article 4 (2) GDPR.

2.2.3 Definition of Controller and Processor – Article 4 (7) and (8)

A controller is defined as a natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.[36] The definition provided is that there is no limitation on the type of entity capable of performing the role of controller.[37] In the event of an infringement, it is the organisation as such that is held liable for the incident, which is also likely to be the case where the organisation has appointed a responsible natural person.[38] Controller arises when the organisation exercises decision-making power by determining the purposes and means of the processing.[39] The decisive factor in determining whether there is a sole or joint controller is whether the organisation itself or jointly with another party has determined the purposes and means of the processing.[40] Whereas the allocation of responsibilities to joint controllers may vary from case to case depending on the stage at which each organisation is involved in the processing.[41]

The existence of sole or joint liability has been determined, inter alia, in cases before the CJEU, known as the Fashion ID.[42] In the present case, the websites/forums of two web operators were integrated with each other, with the Court ruling on the question of joint controller. The decisive factor in the question of whether a joint or individual personal data controller exists is whether the purpose and means of the processing have been determined alone by one party or jointly with another.

Examples of when a sole personal data controller is actualised:

> A company decides to engage in direct marketing by sending emails to potential customers, offering its services therein. In order to carry out this type of marketing, the company must collect email addresses and then send out the said email.
>
> The Company has hereby determined the purpose of the processing by deciding on the processing of email addresses for the purpose of sending emails, including marketing. Furthermore, they have determined the means of processing, with the processing obtaining email addresses from a certain source, storing them, and subsequently using them to contact potential customers.

A processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.[43] The definition of processor has a similar broad meaning as to which entity can assume the role.[44] In order for an organisation to qualify as a processor, it must be a separate entity from the controller, processing personal data on behalf of the controller.[45] When the controller engages

[36] See Article 4 (7) GDPR and EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[37] See EDPB 07/2020 paragraph 17.

[38] Ibid. paragraph 18.

[39] Ibid. paragraphs 20 and 32.

[40] Ibid. paragraph 31.

[41] See Judgement of 5 June 2018 in Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstien GmbH,* EU:C:2018:388, paragraph.43.

[42] See Judgement of 29 July in Case C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV.,* EU:C:2019:629.

[43] See Article 4 (8) GDPR.

[44] See EDPB 07/2020 paragraph 73.

[45] Ibid. paragraph 76.

a processor for the performance of certain personal data processing, a data processing agreement is required in accordance with Article 28 (3) of the GDPR.

Examples of when a controller engages a processor:

> Company A decides on a personal data processing process, which means that they will process email addresses for the purpose of direct marketing through so-called newsletters. Company A chooses to hire the marketing agency Company B, which will collect email addresses and administer newsletter mailings. Company A assumes the role of controller as they determine the purpose (why) and means (how) of the personal data processing. Company B subsequently assumes the role of data processor when they are to perform the processing operation on behalf of Company A.

2.3 General Principles – Article 5

The principles that the controller must comply with when processing personal data are set out in Chapter Two of the GDPR. Furthermore, the fundamental principles are set out in Article 5 (1) of the GDPR. In contrast, the second paragraph of the article stipulates that the responsibility for compliance with the first paragraph lies with the controller. The controller must ensure compliance with the fundamental principles and an obligation to demonstrate such compliance. The controller's liability can only be relieved when the law provides for some relief regarding the processing of personal data. It is not possible for the data subject to consent to a deviation from compliance with the Principles, as consent can never have such a liberating effect.

Purpose limitation principle – Article 5 (1) (b)

The principle of purpose limitation[46] requires that the purpose must be stated expressly and precisely before the collection of personal data begins. The purpose of the processing of personal data must be both clear and legitimate, and they must also be specific, meaning that they must not be too general.[47] The purpose for which personal data are processed must be legitimate, meaning that the processing must be supported on a legal basis and in accordance with other legislation.[48] Where personal data collected by the controller is to be processed for a purpose other than that for which it was collected, this may only be done if the new/different purpose is compatible with the original purpose.

Data minimisation principle – Article 5 (1) (c)

In accordance with the principle of data minimisation[49], the personal data subject to processing must be adequate and relevant to the purpose.[50] The stipulated means that the personal data processed must be necessary to fulfil the purpose, which is

[46] DA: Formålsbegraensning. DE: Zweckbindung. EN: Purpose Limitation. FR: Limitati on des Finalités. SV: Ändamålsbegränsning.

[47] See Öman, Sören. *GDPR (GDPR) m.m. – En kommentar.* 2th ed., Stockholm: Norstedts Juridik, 2021. [Cit: GDPR-En kommentar] page. 124.

[48] See WP 203. 00569/13/EN. *Opinion 03/2013 on purpose limitation.* Adopted 2013-04-02. page. 19.

[49] DA: Dataminimering. DE: Datenminimerung. EN: Data minimisation. FR: Minimisati on des données. SV: Uppgiftsminimering.

[50] See Recital 39 GDPR.

why a certain proportionality assessment should be intended. Thus, the processing must not be too extensive and more personal data than necessary must not be processed. Thus, according to Öman, it must be assessed that the processing satisfies the objectivity requirement, which the controller must verify.[51]

Accuracy principle – Article 5 (1) (d)

The principle of accuracy[52] imposes on the controller a kind of activity requirement, namely that it must actively work to ensure that the personal data processed are accurate and up-to-date if the purpose so requires.[53] The personal data does not necessarily need to be updated unless it is necessary to achieve the prescribed purpose of the processing. In the case of ongoing marketing, it is probably necessary to keep the personal data updated in order for the marketing to reach the right person, while in the case of a one-off mailing, such a necessity does not exist. There is probably a connection between when personal data is incorrect according to the principle of accuracy and when the data is also considered irrelevant according to the principle of data minimisation.[54] As a result of that principle, the controller must take all reasonable steps to ensure that inaccurate personal data processed are either rectified or erased without delay. The data subject also has the right to request this according to Articles 16 and 17 of the GDPR. However, it is worth mentioning that the rights are conditional. The measures that may be considered reasonable may be determined on a case-by-case basis, in which case the nature of the personal data and the effect of its inaccuracy may be taken into account in the assessment.

Storage limitation principle – Article 5 (1) (e)

The principle[55] provides that personal data may be retained (stored) only for as long as is necessary in relation to the purpose for which they were collected. When the storage of personal data is no longer necessary, it must be de-identified or deleted.[56] As a result of this principle, the controller should introduce different time limits on the basis of which a deletion is carried out for the purpose of deleting or de-identifying personal data that are no longer necessary to be retained.[57] The article also provides an exception to the principle whereby personal data may be stored for longer than necessary where processing is carried out for archiving purposes in the public interest, scientific or historical purposes, or statistical purposes, provided that appropriate safeguards have been taken. The exception is not likely to apply when processing takes place for the purpose of direct marketing.

> The CJEU has stated that the storage period of an exam should be assessed in the light of the purpose for which the exam was submitted. The Court did not consider it necessary to retain the personal

[51] See GDPR-En kommentar, pages 134 – 135.

[52] DA: Rigtighed. DE: Richtigkeit. EN: Accuracy. FR: Exactitude. SV: Riktighet.

[53] See GDPR-En kommentar, page 140.

[54] Ibid. page 140.

[55] DA: Opbevaringsbegraensning. DE: Speicherbegrenzung. EN: Storage Limitation. FR: Limitation de la conservation. SV: Lagringsminimering.

[56] See Krzysztofek, Mariusz. *GDPR: Personal Data Protection in the European Union.* 114th ed., Netherlands: Wolter Kluwers, 2021. [Cit: GDPR: Personal Data Protection in the European Union] page. 68.

[57] See Recital 39.

data, the test and personal notes until the end of the examination procedure and the expiry of the appeal period.[58]

Integrity and confidentiality principle – Article 5 (1) (f)

According to principle[59], personal data must be processed to ensure the data´s protection. The principle is clarified in Article 32 of the GDPR, which provides for appropriate measures that can be taken for the more secure processing of personal data. When processing personal data, the controller may consider, for example, backing up the personal data in the event of accidental deletion or disappearance, encryption to protect the personal data in the event of unlawful intrusion or hostage, and organisational measures such as authorisation systems, password management and Wi-Fi connection procedures.[60]

Accountability principle – Article 5 (2)

The principle of accountability[61] means that the controller has ultimate responsibility for ensuring that its processing of personal data is carried out in accordance with all the provisions of the GDPR.[62] Regardless of whether a personal data processor is used, this responsibility cannot be delegated. In addition to the liability mentioned above, there is also a burden of proof, consisting of the fact that it is the controller's responsibility to demonstrate compliance with Article 5 (1) of the GDPR.

Fairness principle – Article 5 (1) (a)

The principle of fairness[63] should not be confused with the principle of accuracy, the terminology of which may give rise to some confusion. The principle of fairness refers to the controller's conduct towards the data subject.[64] I would agree with Öman's position that the Danish, French, German and English versions more clearly indicate the meaning of the principle and thus that a balancing of interests must be carried out.[65] The assessment that can be deduced from the principle can be described as a balancing of interests or a balance of reasonableness. The balancing exercise determines whether the processing is unfair to the data subject.[66] In doing so, the data subject's expectations regarding the processing must be considered in relation to the information provided by the controller.

The principle takes into account, to a large extent, the information assigned to the data subject. The information may be communicated through, for example, policy[67]

---

[58] See Judgement of 20 December 2017 in Case C-434/16, *Peter Nowak v Data Protection Commissioner,* EU:C:2017:994, paragraph 55.

[59] DA: Integritet og fortrolighed. DE: Integrität und vertraulichkeit. EN: Integrity and Confidentiality. FR: Integrité et Conficentialité. SV: Integritet och konfidentialitet.

[60] See Article 32 and Recital 83 GDPR.

[61] DA: Ansvarlighed. DE: Rechenschaftspflicht. EN: Accountability. FR: Responsabilité. SV: Ansvarsskyldighet.

[62] See Kuner, Christopher, A. Bygrave, Lee and Docksey, Christopher. *The EU General Data Protection Regulation (GDPR) – A Commentary.* Oxford: Oxford University Press, 2020. [Cit: GDPR-A Commentar] page 318.

[63] DA: Rimeligt. DE: Treu und Glaube. EN: Fairly. FR: Loyaaté. SV:Korrekt.

[64] See Michael Holtz, Hajo and Ledendal, Jonas. Överlappningen mellan dataskydd och marknadsrätt – GDPRs tillämpning på marknadsföring och marknadsrättens tillämpning på kommersiell personuppgiftsbehandling. *Svensk Juristtidning.* SvJT 2020 s. 143. [Cit: Holtz and Ledendal] page. 4.

[65] See GDPR-En kommentar, page. 121.

[66] Compare Recital 39.

[67] Could be named Privacy Policy or Integrity policy.

and where the processing of personal data is not compatible with the information provided by the controller in its policy, this is to be considered a violation of the principle of accuracy.[68]

In the balance of reasonableness, circumstances such as the data subject's possible right to object to the processing, available information about the processing and the balance of power between the data subject and the data controller must be taken into account.

According to guidelines from the EDPB, a change of legal basis may result in an unfairness incompatible with the principle of accuracy. This may be the case, for example, where the controller processes personal data on the basis of the legal basis performance of the contract, pursuant to Article 6 (1) (b) GDPR, on the basis of a contract between the data subject and the controller, after which the contract is terminated. After the termination of the contract, with certain exceptions, the legal basis of the contract will no longer be reasonable to base the processing on because there is no longer an contract to be performed.[69] When the controller continues to process the data subject's personal data on the basis of a new legal basis, this is a procedure that is unlikely to be expected of the data subject and is therefore unreasonable. The data subject did not expect their personal data to be processed for any purpose other than the performance of a contract.

Transparency principle – Article 5 (1) (a)

The principle of transparency indirectly refers to the controller's compliance with the requirements of Articles 12 to 15 GDPR regarding information for the data subject.[70] The principle means that information and communication between the data subject and the controller must be easily accessible and easily understandable. The information must be provided in clear language in order to establish the best possible understanding on the part of the data subject.[71] The principle of transparency is well linked to the principle of accuracy, as the information is of importance to the expectations of the data subject. Thus, in case of lack of information and transparency, a substandard understanding and expectation is established on the part of the data subject, which can imply a violation of both principles. The information must clearly and unambiguously convey how the data is collected and what processing the data is subject to.

According to the guidelines of the Article 29 Working Party, the principle entails obligations mainly on three levels:

I. How the data subject receives information about the processing or processing carried out,

[68] See GDPR-En kommentar, page 122.
[69] See EDPB Guidelines 2/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, paragraphs 38 – 43.
[70] DA: Gennemsigtighed. DE: Transparenz EN: Transparent. FR:Transparence. SV: Öppenhet.
[71] See Recital 39.

II. What communication is established between the data subject and the controller in light of the rights provided for in the GDPR and

III. How the controller works to facilitate the exercise of the rights of the data subject.[72]

Article 12 of the GDPR provides that the controller must provide clear and precise information under Articles 13 and 14 of the GDPR, while facilitating the exercise of the data subject's rights under Articles 15 to 22 of the GDPR, in the context of the obligation to provide information, in particular Article 15 of the GDPR.

Articles 13 and 14 of the GDPR stipulate what information the controller is required to provide to the data subject. When the personal data has been collected from the data subject, Article 13 applies, while Article 14 applies when the personal data has been obtained from a party other than the data subject. In accordance with Article 15, the data subject has a right of access to information, and thus constitutes a right which must be invoked at the request of the data subject.

2.4 Lawfulness Principle – Article 5 (1) (a)

The principle of lawfulness[73] as set out in Article 5 (1) (a) GDPR must be read in conjunction with Article 6 (1) GDPR in order to understand its meaning. From the wording of Article 5 (1) (a) GDPR, it can be deduced that personal data shall be processed lawfully in relation to the data subject. In addition, the first sentence of Article 6 (1) GDPR provides that the processing of personal data is lawful only if it is based on at least one of the six legal bases. In my view, the principle of lawfulness must therefore be understood as a requirement that the controller has a legal basis justifying the processing of personal data.

As far as Sweden is concerned, preparatory work and case law have interpreted the principle in such a way that a legal basis must justify the processing. Thus, the principle does not imply a broad interpretation of the concept of legality, so that, according to that principle alone, the processing must be compatible with other legislation.[74]

There should be a theoretical possibility of making such a broad interpretation that the terminology "lawfulness" can be understood as meaning that the processing must be compatible with the GDPR and other applicable legislation.[75] In the Swedish comment by Mr Öman, a position is presented by Douwe Korff who believes that in order to be lawful, processing must comply with both GDPR and other legislation.[76] This is also the view of Mr Krzysztofen, who believes that this principle means that the processing must not only comply with the provisions of the GDPR but also

[72] See WP 260 rev.01. 17/EN. *Guidelines on transparency under Regulation 2016/679.* Adopted 2017-11-29, page. 4, which is confirmed in EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation. .

[73] DA: Lovlighed. DE: Rechtmässigkeit. EN: Lawfulness. FR Licéite. SV: Laglighet.

[74] See Prop. 2017/18:105 *Ny dataskyddslag,* page 47. See GDPR-En kommentar, page 119. See HFD 2016 ref. 40.

[75] See Holtz and Ledendal, pages 4 – 5.

[76] See GDPR-En kommentar, page 120.

comply with other applicable laws and regulations.[77] However, as explained above, my view is that the legislature did not intend for a broad interpretation of the principle of lawfulness.

In order to comply with the principle of lawfulness as set out in Article 5 (1) (a) GDPR, the processing must be supported on a lawful basis. The legal bases available are stipulated in Article 6 (1) GDPR, which are consent, contract, legal obligation, vital interest, public interest and legitimate interest. The list in the Article is exhaustive and Member States do not have the possibility to provide for additional legal bases in national law.[78] It follows from the first subparagraph of Article 6 (1) of the GDPR that at least one condition (including a legal basis) must be fulfilled in order for the processing to be lawful.[79] There is no legal obstacle to supporting the processing on more than one legal basis, but it should be noted that a change of legal basis when a legal basis ceases may constitute an infringement.[80]

As regards processing carried out by a private undertaking for the purpose of direct marketing, I consider three of the six legal bases possible to support such processing.

Since the starting point is when a non-public controller performs the processing, the legal basis of public interest cannot be used. Nor is there any legal obligation justifying processing, so that this legal basis is not applicable. Moreover, the processing for direct marketing purposes does not constitute processing which is necessary for the life and health of a person.

The controller wishing to carry out such processing must therefore rely on one of the other three legal bases. Consequently, the data subject's consent to the processing is required, that the processing is necessary for the conclusion or performance of a contract, or when the legitimate interest of the controller outweighs the interest and fundamental rights and freedoms of the data subject.

[77] See GDPR: Personal Data Protection in the European Union, page 55.

[78] See C-582/14 *Patrick Breyer v Bundesrepublik Deutschland,* paragraphs 57–63.

[79] See Prop. 2017/18:105 *Ny dataskyddslag,* page 46. Judgement of 11 December 2019 in Case C-708/18, *TK v Asociatia de Proprietari bloc M5A-ScaraA*, ECLI:EU:C:2019:1064, paragraphs 37 and 53. Judgement of 8 September 2011 in Joined Cases C-68/10 and 58/10, *Monsanto SAS and Others v Ministre de l'Agriculture et de la Pêche*, ECLI:EU:C:2011:552, paragraph 30. C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado.* paragraph 30. C-582/14 *Patrick Breyer v Bundesrepublik Deutschalnd* paragraph 57.

[80] See Article 17 (1) (b) GDPR and Prop. 2017/18:105 *Ny dataskyddslag,* page 46.

3 Performance of Contract

3.1 Introduction

In the event that the controller does not support the processing of personal data on consent or legitimate interest, it may support the processing on the legal basis of *performance of a contract*, as set out in Article 6 (1) (b) GDPR. The legal basis justifies processing which is necessary for the entering to or performance of a contract. Thus, the basis can be used as support for processing that is necessary for the conclusion of a contract when the action is required by the data subject. Furthermore, the ground justifies processing that is necessary for the performance of a contract that has been concluded.

3.2 Requirement for Necessity

What constitutes a necessity is debated and even difficult to generalise.[81] According to the statement of the Court of Justice, 'necessity' is an autonomous concept of Community law which must be interpreted uniformly throughout the EU.[82] Furthermore, the necessity of the processing shall be interpreted in conjunction with the principle of data minimisation as set out in Article 5 (1) (c) GDPR.[83] Since the purpose of a processing can be achieved by other less privacy-intrusive means, the necessity requirement is not likely to be fulfilled.[84] This should not be understood as meaning that the requirement of necessity can only be achieved when no other means are available or where there must be an impossibility of fulfilling the purpose without the processing at hand.[85] The controller may make a balance and a kind of reasonableness assessment if there are other reasonable approaches. In my view, a less intrusive approach, which entails a significantly higher cost, together with a more complex procedure, may not seem to be a reasonable alternative in all situations. Consequently, I consider that necessity must be examined in the individual case and the circumstances associated with it.

The interpretation as to whether a processing is necessary for the performance of the contract must be interpreted strictly, requiring a genuine necessity for the processing to be considered lawful.[86] It is not sufficient that a processing is covered by a contractual term, as such a condition does not automatically create a necessity for the performance of the contract. Rather, such a contractual term must be regarded as a means of imposing non-essential processing on the data subject by means of the

[81] See GDPR-En kommentar, page 159.

[82] See Judgement of 16 December 2008 in Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland,* ECLI:EU:C:2008:724, paragraph 52.

[83] See C-708/18, *TK v Asociatia de Proprietari bloc M5A-ScaraA,* paragraph 48.

[84] See Recital 39 GDPR.

[85] See SOU 1997:39 *Integritet 'Offentlighet' Informationsteknik.* Page 359.

[86] See EDPB 2/2019, paragraph 28.

contract. The essential thing is that the conditions must be met to fulfil the core content of the agreement.

The necessity for the performance of a contract can be illustrated by the following example:

> A consumer A enters into a purchase contract for the purchase of a sofa with company B. The contract stipulates that the company must deliver the sofa to the consumer's home address, and the contract also stipulates that the company may contact the consumer for marketing purposes. In this context, the company can support the processing of the consumer's address and contact details in order to enable the delivery of the sofa on the legal basis of the contract. The sofa and its delivery constitute the core content of the contract, and the processing is, therefore, an absolute necessity for the performance of the contract. Apart from the fact that the marketing term is of such general terms that make it unacceptable, it is also not necessary on which the performance of the contract depends.

3.3 Nature of the Contract

The contract must be valid under contract law in accordance with the Member State's national contract law and other applicable legislation.[87] For example, the terms of a consumer contract must comply with the applicable law; for example, the national legislation implementing Directive 93/13/EEC[88] must be compatible with the content of the contract. A contract which is void under civil law cannot justify processing on the basis of that legal basis. In this context, the individual's ability to act must be taken into account from a legal perspective, whereby a child (generally under 18 years of age) has a limited ability to enter into legally valid agreements. In order for a contractual term to entitle the controller to carry out a processing, the term should be specified and thus not too general. According to guidelines from the EDPB, general terms of processing, such as processing for marketing purposes, are unlikely to be accepted.[89]

3.4 The difference between consent and acceptance of contract terms

It is important to understand the difference that exists between the data subject's acceptance of a contractual term and his or her consent to processing.[90] The difference is expressed partly in the procedure of the expression of the wishes and partly in the consequences that follow from the form of the declaration of wishes as regards the way in which the controller is to provide information and what rights are granted to the data subject. Where the controller seeks to process personal data that is necessary for the performance of a contract on the basis of consent, this does not appear appropriate.[91] Conversely, the EDPB does not consider it appropriate to seek to process personal data that is not necessary for the performance of a contract on

[87] See EDPB 2/2019, paragraph 9.
[88] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[89] See EDPB 2/2019, paragraph 16.
[90] Ibid., paragraph 20.
[91] Ibid., paragraph 19.

the basis of the legal basis of contract.[92] Thus, it can be inferred that the controller should not make an attempt to evade the obtaining of consent by incorporating a contractual term with a similar meaning.

It should be recalled of the data subject's opinion on the matter as the data subject intends to accept the terms of the contract and thus expect a processing that is material based on the agreement entered into. The data subject should not expect to give consent within the framework of the agreement for purposes other than the performance of the agreement.

3.5 Necessary for the Performance of a Contract

As mentioned, the processing must be necessary for the performance of a contract. It is required that the data subject is a contracting party and that the controller is itself a contracting party or performs the contract on behalf of another party.[93] It follows naturally from the requirement that the data subject must be a contractual party, and the controller cannot conclude the contract in question with a legal person.[94]

The performance of the contract is essential, and the burden of proof is on the controller to prove that the main purpose of the contract cannot be achieved other than through the processing in question.[95] It is not relevant whether the processing entails a benefit or not for the data subject.[96]

3.6 Necessary for Entering into a Contract

The legal basis may also justify processing necessary for the adoption of a measure required by the data subject prior to the conclusion of a contract. The following conditions must be met: The data subject must have made a request which requires processing, which is necessary for the implementation of the request. There are no formal requirements for the request to be made, which is why it can be done orally, in writing or by means of a conclusive action (in which case the data subject's wishes are expressed by an action that is not of an oral or written nature).[97] In that regard, it should be borne in mind that it is not necessary for the data subject to intend to conclude an actual contract but only a request for action.[98] The request may, for example, consist of a request for whether a contract can be entered into, in which case the controller has to investigate certain circumstances that require the processing of personal data.

[92] Ibid., paragraph 19.

[93] See GDPR-En kommentar, page 164.

[94] Ibid.

[95] See Judgement of 4 July 2023 in Case C-252/21, *Meta Platforms and Others (Conditions generales d utilization d'un reseau social),* ECLI:EU:C:2023:537, paragraph 98.

[96] See C-252/21, *Meta Platforms and Others (Conditions generales d utilization d'un reseau social),* paragraph 99.

[97] See GDPR-En kommentar, page 167.

[98] Ibid., pages 167 - 168.

3.7 Personalisation in the performance of contracts

Where the data subject enters into a contract for a digital service, such as access to a social network, it has been made clear in guidelines that personalisation is not a necessity, even though it may have positive consequences.[99] To the extent that the data subject's agreement on the functioning of a service may not work optimally, personalisation is not a necessity as the service does work.[100] For example, if a data subject enters into an agreement for a music streaming service, the agreement with the platform may justify the processing of personal data in order to be able to carry out billing for the service. Such information, such as payment information, is therefore a necessity for the performance of the contract. In order for the service to function appropriately, the streaming service wants to offer personalised recommendations for music that suit the data subject, which is a form of marketing that encourages the use of the service. Such processing and analysis of the registered interaction in the service and liking of music are not likely to constitute a necessity for the performance of the contract. This is because the data subject has the full opportunity to listen to the music they want without such an analysis. The agreement can thus be fulfilled without personal offers being presented to the data subject.

3.8 A secure legal basis for the Controller

In my view, that legal basis is fairly secure on the part of the controller. This is because the data subject does not have the right to object to the processing, which means that the processing shall only cease when the agreement is declared invalid, terminated or when the agreement has been fulfilled. Thus, the data subject does not have the right to terminate the processing on his or her own initiative, which constitutes security for the controller against the comparison of consent that can be withdrawn at any given time.

3.9 Summary

In summary, it can be stated that it is the responsibility of the controller to demonstrate the following:

- That an agreement exists,

- That the contract is valid in accordance with national contract law and

- That the processing is objectively necessary for the performance of the contract

It is my firm opinion that this basis is not suitable for supporting a discussion on direct marketing. It would be very difficult, if not impossible, that direct marketing would constitute such a necessity for the performance of a contract. When the idea arises of entering into a contract in which the data subject agrees to have direct

[99] See EDPB 2/2019, paragraphs 51 – 53.
[100] Ibid., paragraph 57.

marketing sent to him, this should express a consent rather than a necessity for the performance of a contract.

4 Legitimate Interest

4.1 Introduction

At the outset, the legal basis of legitimate interest can be described as a legal basis, which, in my view, is a general legal basis which may justify a large amount of processing of personal data which cannot be supported on any of the other legal bases. Mr Öman describes the legal basis in terms of the terminology 'a general clause',[101], which, in my view, implies a certain truth in relation to its practical application. A general view of legitimate interest would be that the legal basis is a slush funnel or a last resort that should only be used where no other legal basis is applicable.[102] I do not agree with such a view, as I consider that legitimate interest, like the view of the Article 29 Working Party, has the same high legal status as the other legal bases.[103] Legitimate interest should not be seen as a last resort but as an alternative, like the other legal bases, which can be used primarily depending on the nature of the processing.

The case law has set out three cumulative conditions for the application of a legitimate interest:

- A legitimate interest of the controller or a third party must be pursued in the exercise of the processing;
- The processing must be necessary to satisfy the legitimate interests, and
- The interests and fundamental rights and freedoms of the data subject shall not outweigh the legitimate interest of the controller or of a third party.[104]

4.2 General Conditions for Legitimate Interest

As explained in the introduction to this section, the legal basis of legitimate interest can be based either on the legitimate interest of the controller or on the part of a third party.[105] Thus, an initial purpose is required for personal data processing, which is based on a legitimate interest. On the basis of guidance provided by the Article 29 Working Party, 'legitimate interest' should be interpreted more broadly than 'legitimate purpose.[106] Thus, it may appear that the controller is recognised as having a legitimate interest, which cannot, on the other hand, be regarded as a legitimate purpose. This may happen, for example, when the controller has an acceptable

[101] See GDPR-En kommentar, page 181.

[102] See WP 217, page 9.

[103] Ibid., pages 9 – 10.

[104] See C-252/21, *Meta Platforms and Others (Conditions generales d utilization d'un reseau social),* paragraph 106, with reference to C-597/19, *Mircom International Content Management & Consulting (M.I.C.M) Limited v Telenet BVBA,* paragraph 106.

[105] See WP 217, page 23.

[106] Ibid., pages 24 – 25.

interest (sending an offer to a consumer to offer them cheaper goods (direct marketing)). In contrast, the purpose for which the interest is to be fulfilled is not considered acceptable/legitimate (to enable the sending of relevant offers, the company will monitor the consumer's eating habits, interaction on different websites, tracking of location, etc.). In order to be considered legitimate, the interest must be compatible with the relevant legislation for the processing, and in doing so, legislation must be interpreted broadly so that most national laws may be applicable and thus need to be taken into account.[107] Furthermore, a legitimate interest must be sufficiently clear and specific to allow a balance to be struck, while at the same time, it must be a genuine and actual interest, which means that it must not be a speculative interest.[108]

The Article 29 Working Party has published in its guidance a non-exhaustive list of interests which, in its opinion, are legitimated:

- "exercise of the right to freedom of expression or information, including in the media and the arts
- **conventional direct marketing and other forms of marketing or advertisement**
- unsolicited non-commercial messages, including for political campaigns or charitable fundraising
- enforcement of legal claims including debt collection via out-of-court procedures
- prevention of fraud, misuse of services, or money laundering
- employee monitoring for safety or management purposes
- whistle-blowing schemes
- physical security, IT and network security
- processing for historical, scientific or statistical purposes
- processing for research purposes (including marketing research)"[109]

In the second point, the list states that direct marketing constitutes a legitimate interest, which is also provided for on the Swedish supervisory authority's website.[110] The mere fact that direct marketing is mentioned as a legitimate interest does not mean *per se* that the processing in the individual case will be permissible after an overall assessment in the form of a balancing of interests.

4.3 The Interest of Third Parties

The legal basis may also be applied to processing for the legitimate interest of a third party, in which case the controller does not actually have a legitimate interest in

[107] See WP 217, page 25.
[108] Ibid., page 24.
[109] Ibid., page 25. (Author's bold)
[110] See Integritetsskyddsmyndigheten. Intresseavvägning. 2021-09-15 <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/intresseavvagning/> (Accessed 2024-05-22). This is also evident from Recital 47 GDPR.

processing the personal data.[111] The procedure then looks like the controller carries out the processing of personal data, in which case a third party has an interest. An illustrative example to explain how such a situation can be expressed can be found in the guidance of the Article 29 Working Party.[112] It describes a situation in which an undertaking publishes salary data on members of its management, in which case there is no legitimate interest in the controller (the undertaking). On the other hand, employees and journalists (third parties) have a legitimate interest in accessing the data in order to exercise scrutiny of the company's management.

4.4 Requirement of Necessity

As explained in the legal basis for the performance of a contract, there is also a requirement of necessity.[113] The processing of personal data must be necessary to satisfy the legitimate interest of the controller or a third party.[114] The necessity requirement is something that, in my opinion, should be given great attention when assessing whether the processing is lawful. Alternative processes that are less invasive of privacy should be applied if they are available.

4.5 Interest of Data Subject

In the balancing of interests, the interests and fundamental rights and freedoms of the data subject must be taken into account. Initially, it should be noted that the wording of the interests of the data subject is absent from the concept of justified. Thus, it is not necessary for the interest of the data subject to be legitimate, but all interests must be taken into account in so far as they are relevant to the case at hand.[115] As we are in a modern world where the flows of personal data are of an enormous nature, it is of the utmost importance to show consideration for the data subject's interest in not being subject to processing. In that regard, I consider it appropriate to reproduce the Article 29 Working Party's guidelines as follows:

> ”Even individuals engaged in illegal activities should not be subject to disproportionate interference with their rights and interests. For example, an individual who may have perpetrated theft in a supermarket could still see his interests prevailing against the publication of his picture and private address on the walls of the supermarket and/or on the Internet by the owner of the shop.”[116]

The above-cited demonstrates the broad interpretation of the interest of the data subject.[117]

Furthermore, it seems natural to me that a broad interpretation should be given to the interests and fundamental rights and freedoms of the data subject. Not implementing

[111] See WP 217, page 27.
[112] Ibid., pages 27 – 28.
[113] Ibid., page 29.
[114] Ibid., page 29.
[115] Ibid., pages 29 – 30.
[116] Ibid., page 30.
[117] Ibid., page 29.

a broad interpretation would be contrary to the purpose of the Regulation according to Article 1 (1) GDPR. As far as the rights guaranteed to citizens in the EU are concerned, it should be a principle to carry out a broad interpretation of the right itself. In that regard, it should be recalled that exceptions or limitations to the general rule relating to the protection of the data subject's private life and fundamental rights and freedoms must be interpreted strictly.[118]

4.6 Balancing of Interests

The assessment required by Article 6 (1) (f) GDPR can be referred to as a balancing test or a balancing of interest. It does not seem decisive that the controller has a legitimate interest at the same time as the data subject has his or her interests and his or her right to fundamental rights and freedoms. As provided for in the article, it is decisive, for the lawfulness of the processing, that the legitimate interest trumps the interests and fundamental rights and freedoms of the data subject (or as it is provided for, "[...] legitimate interests, unless the interests of the data subject **or** (emphasis added) fundamental rights and freedoms outweigh them and require the protection of personal data, in particular where the data subject is a child."[119]). It should be noted that the provision provides for 'or', which means that it is sufficient that the interests of the data subject are considered to outweigh the legitimate interest in order for the processing not to be regarded as lawful. In order for the controller to come to a conclusion as to whether the processing is lawful or not, it is required that it carries out a balancing of interests.

The balancing of interests must consist of an assessment of the overall outcome of the processing.[120] Rarely should the legitimate interest alone be considered to outweigh the interest and fundamental rights and freedoms of the data subject. Other circumstances, such as the amount of personal data planned to be processed, the nature of the personal data, the planned safeguards and the retention period appear to be decisive for the outcome of the balancing of interests.[121]

[118] See Judgement of 16 Decemeber 2008 in Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy,* ECLI:EU:C:2008:727, paragraph 56.

[119] See Article 6 (1) (f) GDPR.

[120] See Judgement of 24 September 2019 in Case C-136/17, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL),* ECLI:EU:C:2019:773, paragraph 66.

[121] See WP 217, pages 30 – 31.

To illustrate how a balancing of interests can be made, this can be likened to a balance of scales, as shown in the following example:

Left Scale *Controller*	**Right Scale** *Data subject*
- Legitimate interest - Necessity of the processing - Safeguards - The Data Subjects possibility to op-out	- Interest - Fundamental rights and freedoms - Reasonable expectations - Consequences of the processing

The various scales must then be weighed against the existence in order to deduce the outcome and then determine whether the processing can be considered lawful under this legal basis.[122]

I: Initially, an assessment must be made regarding the controller's legitimate interest. Thus, what is subject to assessment is the nature and necessity of the legitimate interest.[123] For example, if the interest consists in the exercise of a fundamental right, if there is a public interest in the processing or if the interest is of a different nature.[124] The requirement that the processing must be necessary and proportionate in relation to the fulfilment of the legitimate interest has been described previously.[125]

II: After determining the legitimate interest, the controller must assess the potential consequences that may affect the data subject, both in a positive and negative sense.[126] When determining positive consequences, this may speak in a favourable direction for the controller. For example, the marketing that is planned to be conducted will benefit the data subject. As regards the negative consequences, particular consideration must be given to whether the data subject may suffer harm through exclusion from context, discrimination, risk of being slandered, suffer a loss of reputation or be otherwise harmed.[127] Especially when marketing, it is essential to consider the emotional consequences such as irritation, increased sadness, fear or stress that may affect the data subject. The feeling of being tracked or monitored can also cause discomfort for the data subject, which must be taken into account.

For example, marketing for a service relating to the disposal of household goods after death may cause increased grief and irritation for the data subject who is grieving for a recently deceased loved one.[128] Even though the negative

[122] See WP 217, pages 33 – 34.
[123] Ibid., page 34.
[124] Ibid., pages 34 – 36.
[125] Ibid., page 34.
[126] Ibid., page 37.
[127] Ibid., page 37.
[128] See GDPR-En kommentar, page 190.

consequences, such as discrimination, are unlikely to occur, I believe that the emotional consequences strongly indicate that such marketing does not seem appropriate in this context.

When assessing impacts, both potential and actual impacts must be taken into account by the controller; any impact that may affect the data subject must be taken into account in the assessment.[129] One reason for the importance of analysis of all the consequences that may occur is the difficulty of healing and compensating for some consequences afterwards.[130] In this context, for example, the reputation of a deteriorating person may be emphasised, as it is difficult to correct such a consequence retrospectively. In my view, the impact assessment should not be understood as a burden on the controller but rather as an aid in determining what preventive measures can be taken to protect the data subject's privacy.

After the consequences have been identified, the controller has to assess the likelihood of the consequences occurring.[131] Through such an assessment, the controller has the opportunity to reduce the probability through various protective measures. The degree of severity of each consequence is also an important factor in the balancing of interests for the decision on the lawfulness of the processing.[132] I find it particularly important not to consider a larger quantity of data subjects as a factor affecting the outcome.[133] Even where the processing involves consequences for a small number of data subjects, it is nevertheless important for the person or persons that their right to privacy is respected.[134]

I mentioned earlier that the nature of the data plays a significant role in the outcome of the balancing of interests. The nature of the personal data is to be understood if the data can be classified as non-sensitive (e.g. name or e-mail address) or sensitive personal data (e.g. health data or sexual orientation).[135] As the personal data that is processed constitutes sensitive data according to Article 9 of the GDPR, a legal basis in Article 9 (2) must be applied, and processing generally entails that more serious consequences may arise, which places higher demands on safeguards and those of the controller as such.[136] As regards processing carried out for the purpose of conducting direct marketing, no sensitive data should generally need to be processed. That said, an assessment must be made in the individual case (for each processing), as the content of the marketing may be based on, for example, a medical history, which entails the processing of sensitive personal data. In most cases, the data subject's name, address, telephone number and e-mail address are processed, which do not constitute sensitive personal data.

The controller must also take into account how the data will be processed.[137] The fact that there is little personal data that is processed for a legitimate purpose, in

[129] See WP 217, page 37.
[130] Ibid., pages 37 – 38.
[131] Ibid., page 38.
[132] Ibid.
[133] Ibid.
[134] Ibid.
[135] Ibid.
[136] Ibid., pages 38 – 39.
[137] Ibid., page 39.

combination with certain processing, can result in a significant invasion of privacy in the data subject's private life. When the controller combines different personal data with or applies a behavioural analysis, this can have serious consequences.[138]

What expectations are established for the processing of personal data when the data subject provides their personal data? This is a question the controller should consider. When collecting personal data, the controller has the opportunity to create reasonable expectations on the part of the data subject, which subsequently sets the framework for the processing.[139] In doing so, it is necessary to take into account what the data subject can expect his or her e-mail address to be used for when he or she provides the address to a company for the purpose of obtaining marketing. Most likely, the data subject expects the company to send newsletters, which is a reasonable expectation. On the other hand, in my opinion, it does not constitute a reasonable expectation that the company will provide the email address of other companies that, in turn, send out their newsletters, provided that I have not been informed of this.

In the marketing context, a large group of data subjects are likely to be subject to the processing. The balancing of interests must, therefore, be based on the average data subject, meaning that an assessment does not need to be made in relation to each of the data subjects.[140] On the other hand, a reasonable distinction should be made between different recipients of marketing, for example, between contact persons of business customers and consumers, as consumers are subject to specific legislation.[141] When one or more of the registered persons are children, mentally ill or suffer from another condition which puts the person in a deteriorating situation, this must be given special consideration.

Based on what has been explained so far, it may be difficult for the controller to justify lawful processing. The taking of various protective measures is one factor that can make the apparently illegal processing legal. In this regard, it is up to the controller to consider and consult which safeguards, internal and external, have the effect of mitigating or nullifying the consequences for the data subject.[142]

4.7 The data subject´s right to opt out

With regard to direct marketing, there is a specific provision in Article 21 (2) of the GDPR, which stipulates that the data subject shall at any given time have the opportunity to object to processing carried out for direct marketing. When the data subject objects to the processing, the processing shall cease in accordance with Article 21 (3) GDPR, which is an unrestricted right. In that regard, it must be borne in mind that the possibility of objecting must be as accessible, if not more accessible, as the provision of one's personal data. This possibility of objecting is described as an "opt-out" on the part of the data subject. An opt-out option is usually offered in

[138] Ibid., pages 39 – 40.
[139] Ibid., page 40.
[140] Ibid., pages 40 – 41.
[141] Ibid.
[142] Ibid., pages 42 – 43.

connection with each marketing mailing or marketing contact. The possibility for the data subject to easily object to the processing, which in turn is forced to cease, speaks in favour of the controller. The data subject's ability to influence and have the marketing stop mitigates the negative consequences that may affect the data subject. For example, when the data subject experiences irritation from the marketing, he or she can easily object to the outcome of no longer being subject to the processing.

In the case of Sweden, such an opt-out is offered in advance through a national blocking register for direct marketing[143], where a private individual can register, and thus, a company may not provide direct marketing to the registered person.[144] The fact that the controller consults the register before commencing its direct marketing constitutes such a pre-processing act, which also militates in favour of a favourable outcome from the controller's balancing of interests.[145]

4.8 Selection of Relevant Case Law

4.8.1 Case law from CJEU

4.8.1.1 C-252/21

In its ruling, the CJEU recalled the caution to be exercised when the data subject is a child.[146] A child's personal data deserves special protection because they lack awareness of their rights, the safeguards taken, and the future consequences of being subject to processing.[147] Where the controller chooses to base the processing on legitimate interest, it must inform the data subject of the legitimate interest that gives rise to the processing of the personal data.[148] The CJEU emphasised the requirement of necessity, and therefore, the processing must constitute a strict necessity for the satisfaction of the legitimate interest.[149] According to the CJEU, the controller should consider whether other equally effective but less privacy-intrusive measures/means are available.[150] The requirement of necessity shall be examined in conjunction with the principle of data minimisation as provided for in Article 5 (1) (c) GDPR.[151] The importance of the data subject's reasonable expectations can be deduced from the ruling.[152] Finally, it can be highlighted that the CJEU pointed out that direct marketing and personal advertising constitute a legitimate interest of the controller.[153]

[143] NIX-spärregister. NIX-block register.
[144] See GDPR-En kommentar, page 191.
[145] Ibid., page 191.
[146] See C-252/21 *Meta Platform and Others (Conditions générales d'utilisation d'un reseau social),* paragraph 105 and 111.
[147] See Recital 38 and C-252/21 *Meta Platform and Others (Conditions générales d'utilisation d'un reseau social),* paragraph 111.
[148] See C-252/21 *Meta Platform and Others (Conditions générales d'utilisation d'un reseau social),* paragraph 107.
[149] Ibid., paragraphs 108 and 126.
[150] Ibid., paragraph 108.
[151] Ibid., paragraph 109.
[152] Ibid., paragraph 112 and recital 47.
[153] See C-252/21 *Meta Platform and Others (Conditions générales d'utilisation d'un reseau social),* paragraph 115.

4.8.1.2 C-131/12

A CJEU ruling concludes, unsurprisingly, that a balancing of interests is required in order to support the processing of personal data on legitimate interest.[154] The precondition is thus that the processing is necessary for the purpose which follows from the legitimate interest, and where the legitimate interest outweighs the fundamental rights and freedoms of the data subject and the right to privacy.[155] In that regard, the CJEU recalls that the legitimate interest must be weighed against the right to privacy enshrined in the Charter, as enshrined in Articles 7 and 8 of the Charter of the European Union.[156]

The CJEU presents an interesting line of reasoning, which, in my opinion, should very much be taken into account in a balancing of interests. The impact assessment should be made on the basis of a kind of entity of the processing of personal data. As a result of the circumstances of the individual case, the personal data, in combination with the means of processing, may entail greater consequences and thus entail a serious restriction on the individual's private life. The processing in the present case was carried out by means of the provision of personal data on a search engine, in which case each person who has access to that search engine has access to the personal data. Consequently, a relatively detailed image can be created by a person through a simple search. Without major obstacles, personal data can be linked together and create a structured overview of information about an individual. As a result, and with the contribution of the large access to the internet that exists in today's modern society, there is a risk of serious interference in an individual's private life.[157] Even when a single piece of personal data did not entail any major interference in an individual's private life, the possibility of combining different personal data meant that the interference was greater.

Due to the serious interference with the individual's private life (CJEU's expression), the processing could not be justified solely on the basis of an economic interest on the part of the controller. A balance must be struck between the interest in sharing the information with the public and the fundamental rights and freedoms of the data subject, according to the EU Charter. In the present case, the court considered that the interest of the data subject outweighed the interest of the internet user in accessing the information. However, the outcome of the balancing depends on the type of information to which the processing relates and the type of personal data, sensitive or non-sensitive, that is processed.[158] Thus, it is not a given that processing is not lawful only when, for example, sensitive personal data is processed, but an overall assessment is required.

---

[154] See Judgement of 13 May 2014 in Case C-131/12, *Google Spain SL and Google Inc. v Agencia Espanola de Protección de Datos (AEPD and Mario Costeia González,* ECLI:EU:C:2014:317, paragraph 74.

[155] See Case C-131/12, *Google Spain SL and Google Inc. v Agencia Espanola de Protección de Datos (AEPD and Mario Costeia González,* paragraph 74.

[156] See Case C-131/12, *Google Spain SL and Google Inc. v Agencia Espanola de Protección de Datos (AEPD and Mario Costeia González,* paragraph 74 with maid references.

[157] See Case C-131/12, *Google Spain SL and Google Inc. v Agencia Espanola de Protección de Datos (AEPD and Mario Costeia González,* paragraph 80. With reference to Judgement of 25 October 2011 in Joined Cases C-509/09 and C-161/10, *eDate Advertising GmbH and Others v X and Société MGN LIMITED,* ECLI:EU:C:2011:685*,* paragraph 45.

[158] See C-131/12, *Google Spain SL and Google Inc. v Agencia Espanola de Protección de Datos (AEPD and Mario Costeia González,* paragraph 81.

4.8.1.3 C-708/18

The CJEU began by recalling the necessity requirement, which is common to all legal bases, with the exception of the case of obtaining consent.[159] Consequently, the processing of personal data must be necessary to fulfil the purpose for which the legitimate interest is based. The necessity must be assessed on the basis of the proportionality of the processing in question, including the consideration of alternative measures.[160] Where necessity is to be examined, it must be done in conjunction with the principle of data minimisation, as the amount of personal data subject to processing is an essential factor.[161] In the present case, the controller had considered alternative measures which were not sufficient to achieve the purpose.

The CJEU further expressed that the application of Article 6 (f) of the GDPR is subject to three cumulative conditions:

I. The controller or third party shall carry out the processing of personal data for the purpose of protecting and fulfilling a legitimate interest.

II. The processing of personal data must be necessary to protect and fulfil the legitimate interest.

III. The fundamental rights and freedoms of the data subject shall not outweigh the legitimate interest.[162]

The legitimate interest must be a factual interest at the time of the processing of the personal data and, thus, not a hypothetical one.[163]

The CJEU expressed that a balancing of interests must be carried out in order to determine whether the legitimate interest outweighs the fundamental rights and freedoms of the data subject.[164] In doing so, the circumstances of the individual case must be taken into account. Significant factors in the CJEU's opinion were, on the one hand, the seriousness of the breach of privacy and, on the other hand, whether it is possible to access the personal data in question from publicly available sources.[165] According to the CJEU, it constituted a more serious violation of privacy as the controller, through the processing, gains access to personal data that is not possible to access through publicly available sources.

I agree with the Court's interpretation of Article 6 (f) GDPR to a large extent. However, I do not consider it to be a more serious invasion of privacy *per se* solely because the personal data is not publicly available. Conversely, I do not see it as mitigating as the information is publicly available. For example, I see the processing

---

[159] See C-708/18*, TK v Asociatia de Proprietari bloc M5A-ScaraA,* paragraph 31.

[160] See C-708/18*, TK v Asociatia de Proprietari bloc M5A-ScaraA,* paragraph 49.

[161] Ibid., paragraph 48.

[162] See C-708/18*, TK v Asociatia de Proprietari bloc M5A-ScaraA,* paragraph 40 with reference to C-13/16 *Valsts policijas Rigas regiona parvaldes Kartibas policijas parvalde v Rigas posvaldibas SIA "Rigas satiksme",* paragraph 28.

[163] See C-708/18*, TK v Asociatia de Proprietari bloc M5A-ScaraA,* paragraphs 43 – 45.

[164] Ibid., paragraph 52.

[165] See C-708/18*, TK v Asociatia de Proprietari bloc M5A-ScaraA* paragraph 54 with reference to C-13/16 *Valsts policijas Rigas regiona parvaldes Kartibas policijas parvalde v Rigas posvaldibas SIA "Rigas satiksme",* paragraph 32.

of a data subject's email address that is not publicly available as a very minor violation of privacy. While the processing of a social security number, which, as far as Sweden is concerned, is publicly available, is a very serious invasion of privacy. However, I must agree that it is an essential factor to take into account whether personal data are publicly available.

4.8.2 Swedish case law

4.8.2.1 RÅ 2001 ref. 68

The ruling is a Swedish court case handed down by the Supreme Administrative Court of Sweden in 2001. Despite its age, I do not find the case obsolete, and thus, it is still a precedent within the framework of Swedish law. The case was based on a Swedish company requesting an address register of Swedish milk producers, which was provided by the Swedish Board of Agriculture. The request for disclosure of the register was justified by the Swedish provisions on the right of access to public documents. The purpose of the company's access to the address register was to send direct marketing to milk producers based on the legal basis of legitimate interest.

The Supreme Administrative Court recalled that the processing of personal data for the purpose of conducting direct marketing may be lawful on the basis of legitimate interest. The Court emphasised the data subject's unconditional right to object (object to processing) and that the legitimate interest of the controller slightly outweighs the interest of a data subject who has not objected to processing. Furthermore, the Court found that the processing was considered necessary in relation to its purpose, while at the same time, the purpose was considered to constitute a legitimate interest. Consequently, the court found that the processing to be carried out by the company on the basis of a legitimate interest was lawful and therefore, the Swedish Board of Agriculture could not prevent the disclosure of the address register.

4.8.2.2 RÅ 2002 ref. 54

This case, like the previous one, consists of a decision from the Swedish Supreme Administrative Court. A company which provided student discount cards requested from the Swedish Board of Student Finance (CSN) an extract from its register of recipients of student finance. The company intended to conduct direct marketing, offering discounts to those who study at universities or colleges in Sweden.

The Supreme Administrative Court obtained an opinion from the then supervisory authority in the area, the Swedish Data Protection Authority (which today is the Swedish Authority for Privacy Protection), which expressed that the company's commercial interest in conducting direct marketing outweighed the students' interest in protecting personal privacy.

The Supreme Administrative Court recalled the fact that the purpose set by the company constitutes a legitimate interest. Furthermore, the court found that the company's commercial interest could be considered to outweigh the individual's privacy interest. The data that was processed was not considered to be of a sensitive nature, while the data subject's right to object was highlighted, both of which speak

in favour of the controller. In the opinion of the Supreme Administrative Court, the company appeared to have a legitimate interest, and based on an overall assessment, its legitimate interest was considered to outweigh the interests, fundamental rights, and freedoms of the data subject.

4.8.2.3 KRGBG 3486-20

In this case, which was decided by the Administrative Court of Appeal in Gothenburg, the court had to rule on disclosing personal data for a commercial purpose. A business owner requested access to information about grave rights holders from the Church of Sweden, who came to deny the request on the grounds that the business would not process personal data in accordance with GDPR.

The purpose for which the personal data would be processed was of a commercial nature, in which case the data would be used for the purpose of marketing for grave care services. In the Court's view, the processing appeared to be necessary in relation to its purpose, even when other methods were available. The court justified the necessity on the basis that it was essential for the trader to be able to turn directly to the grave rights holders. My understanding is that the court probably found the information requested in relation to the purpose to be so minor that the necessity requirement was considered to be met. However, I do not believe that the requirement of necessity can be considered fulfilled as there are procedures that are less restrictive of privacy, which is why I do not entirely agree with the Court's reasoning.

I find that there was a legitimate interest on the part of the trader, as the court has held. The Court recalls the balancing of interests that must be carried out, in which case they considered the interests of the data subject to outweigh the result, which is why the outcome was that the processing is not considered lawful.

In the court's reasoning regarding the interest of the data subject, which was found to weigh heaviest, such an overall assessment was presented, which I consider to be correct when applying a balancing of interests. Emotional circumstances such as a death in the near future and the sensitivity of a deceased person's resting place entailed such consequences that spoke in favour of a significant invasion of privacy. In this way, the importance of all circumstances in balancing interests is exemplified. Therefore, the controller cannot assess the lawfulness of the processing solely based on its legitimate interest, the type of personal data processed and the manner in which the processing is carried out, but must make an overall assessment of all relevant circumstances, including the emotional consequences of the exercise of processing.

4.9 Summary

In summary, it can be stated that direct marketing constitutes a legitimate interest of the controller. My opinion is that provisions in the GDPR, together with those stated in both case law and other guidance, indicate that legitimate interest constitutes an appropriate legal basis for direct marketing. The assessment must be made on a case-by-case basis, in which case the controller weighs its legitimate interest against the

interest and fundamental rights and freedoms of the data subject. Provided that appropriate safeguards are taken, the processing only relates to necessary data; the processing is strictly necessary for the performance of direct marketing together with the data subject's possibility to opt-out; all of these should indicate that direct marketing can be supported on this legal basis.

5 Consent of the data subject

5.1 Introduction

Among the legal bases, consent is probably one of the most useful in the context of marketing in general. Why should it be one of the most reversible? I will return later. The definition of consent is found in Article 4 (11) GDPR and should thus be understood as:

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"[166]

Thus, the consent can be given in writing, orally or through a conclusive action.

5.2 Requirement of Necessity

For all of the legal bases in Article 6 (1), with the exception of consent, there is a requirement of necessity. Such a requirement is not provided in the case of consent, so the data subject may consent to the processing of his or her personal data in a completely unnecessary manner.[167] In practice, this means that the controller's burden of proof is lightened as it does not have to demonstrate the necessity of the processing. The advantage in this regard should be that marketing constitutes such a measure which can hardly constitute a necessity so it makes it easier for the controller not to have to make such an argument.

5.3 Conditions for Consent

The data subject must be faced with a clear choice when giving consent, which must follow a genuine and voluntary act on the part of the data subject. It can be inferred from the definition of consent that consent must be given by means of a voluntary, specific, unambiguous and informed act.[168] Thus, the data subject must be aware of what he or she consents to and the subsequent consequences of a given consent.[169] Furthermore, consent must be given voluntarily, which should mean that the data subject should not feel obliged to consent to the processing.[170] A situation in which the data subject may experience such coercion is when he or she is dependent and in a position of power to the controller.[171] Such a relationship typically arises between

[166] See Article 4 (11) GDPR.
[167] See GDPR-En kommentar, page 158.
[168] See Article 4 (11) GDPR.
[169] See EDPB Guidelines 05/2020 on consent under Regulation 2016/679, paragraph 62.
[170] Ibid., paragraphs 13 – 14.
[171] Ibid., paragraphs 21 – 22.

an employer and an employee, in which case consent should be used with great caution.[172]

It follows from Article 7 (2) GDPR that where consent is given by means of a written declaration together with other questions, the question of consent must be presented in a clear and unambiguous manner in order to be distinguishable from the other questions. In doing so, the controller shall use clear, unambiguous and appropriate language in order to establish an understanding on the part of the data subject.[173] A distinctive feature between the consent request and other questions can be implemented with different colour choices or other layouts that clearly demonstrate a difference for the data subject between the question of consent and other questions or information.

Consent must be given through an active act, for example, by giving verbal consent, signing documents, electronic signatures or by the data subject ticking a box. It is clear from the preamble to the GDPR, as well as in case law that pre-ticked boxes do not satisfy the requirement of giving consent.[174] Thus, passive consent cannot be accepted, in which case the data subject must remove the tick from the box only if he or she does not consent to the processing.

By definition, the consent given must be informed, meaning that the data subject must at least be aware of who the controller is and the purpose of the processing.[175] The use of the term, at least in the recital, should emphasise a minimum level of the requirement for information, but the information requirements in Articles 12 to 14 must be observed in order for processing to comply with the principle of transparency.

The burden of proof that consent has been given in accordance with Article 7 (1) GDPR lies with the sole controller or joint controllers. The controller should therefore appropriately store the collected consent through, for example, consent cookie, TC-string, archiving of oral, written or electronic consent.

A further condition for consent to meet the prescribed requirements is that the data subject is given the opportunity to withdraw his/her consent at any given time.[176] This is an absolute right of which the data subject must be informed when giving consent. In accordance with Article 7 (3) of the GDPR, it must be at least as easy to withdraw consent as it was to give it.[177] The stipulated should mean that even when the controller requires written consent, revocation can take place orally, which is a simpler measure than a written notification. In this regard, it should be noted that the burden of proving that a revocation has taken place rests with the data subject. In my opinion, the data controller should make it as easy as possible for the data subject to

[172] See Recital 43 GDPR.

[173] See GDPR: EU Data Protection in the European Union, pages 72 – 73.

[174] See Judgement of 1 October 2019 in CaseC-673/17, *Bunderverband det Verbraucherzentralen unde Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH,* ECLI:EU:C:2019:801, see also Recital 32 GDPR.

[175] See Recital 42 GDPR.

[176] See EDPB 05/2020, paragraphs 112 – 114.

[177] Ibid., paragraphs 112 – 114.

withdraw his or her consent in order to protect the data subject's vulnerability as an individual, in most cases with little knowledge, both legally and technically.

5.4 When the data subject is a child

When processing the personal data of children on the legal basis of consent is based on the legal basis of consent, particular care should be taken on the part of the controller.[178] In doing so, the child's age and intellectual maturity must be taken into account in terms of the information to be provided and whether consent is appropriate. In general, there is no age limit below which the controller can't obtain consent. Such a provision is found only where consent is obtained for information society services. Information society services refer to digital/electronic services provided for remuneration at a distance by an individual request from the recipient of the service, such as social media, search services and apps on smart devices.[179] For such services, according to the main rule in Article 8 (1) GDPR, consent can only be obtained from those who are 16 years of age or older; for younger individuals, consent from guardians is required. The age limit varies from one Member State to another, as Member States can provide for a lower age of 13 years.[180] In the case of Sweden, consent can be given by a person who has reached the age of 13 in accordance with 2:4 of the Data Protection Act (2018:218).

A controller who intends to process personal data and does not provide information society services must consider whether the child has the ability to foresee the consequences of the consent and subsequent processing. It should not be impossible to establish such an understanding through, for example, a visual information video or the like. In my opinion, it should not be appropriate to obtain consent from a data subject whose age is less than 13 years but based on the child's intellectual maturity and understanding of future consequences.

5.5 Direct marketing while using cookies

The e-privacy directive[181] was adopted on 12 June 2002 and has since been implemented in Swedish law through the "Lagen om elektronisk kommunikation" and in Danish law through the" Lov om ændring af lov om elektroniske kommunikationsnet og -tjenester". It follows from the form of a directive in the legal act that each Member State must implement the directive through national law. The Directive aims to harmonise the legal situation within the Union and thereby achieve equivalent protection of fundamental rights and freedoms, in particular, the right to privacy and confidentiality. The Directive lays down rules applicable to electronic communications, which is to be understood as meaning that, according to Article 2 (d):

[178] See EDPB 05/2020, paragraph 124.

[179] See GDPR-En kommentar pages 237 – 238 and Directive 2015/1535 art. 1 (1) (b).

[180] See Article 8 (1) GDPR.

[181] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concering the processing of personal data and the protection of privacy in the electronic communications sector.

> "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information"[182]

The Directive is intended to supplement, according to its Article 2 (2) e-privacy directive, Directive 95/46/EC, which has now been replaced by the GDPR. Thus, the e-privacy directive and the GDPR work in parallel with each other.

Cookies are small text files that are stored on a user's terminal equipment, such as a text file that stores information about a user who visits a website. Cookies are used partly for the website's function, such as providing language settings, and partly for other purposes, such as collecting statistics or information about how a visitor integrates with a website. Cookies can be categorised in different ways, usually between necessary, statistical, functional and analytical. Cookies that provide load balancing, for example, are one such necessary cookie that does not require consent for its use. Consent is required for both tracking cookies and third-party cookies used for behavioural advertising.[183] When using cookies, the e-privacy directive is applied, which sets out the requirements for consent. According to Article 2 (f) of the ePrivacy Directive, consent in the Directive shall correspond to the consent provided for in the processing of personal data in the GDPR, more specifically, Article 7 of the GDPR.

When the data controller chooses to use cookies as a tool to collect information for direct marketing purposes, it must obtain consent. This means that the collection itself requires consent, while other parts, such as the storage of personal data, can be supported on another legal basis. This is important to point out because, depending on how the processing takes place, a legitimate interest is not sufficient when using cookies because a requirement for consent is stipulated.[184]

5.6 Processing of sensitive personal data when conducting direct marketing

Sensitive personal data are prohibited from processing as a general rule in Article 9 (1) GDPR insofar as the processing is to be supported on an additional legal basis in Article 9 (2) GDPR. From Article 9 (1) can be deduced a list of which personal data is of a sensitive nature can, these are personal data that revealed:

> Race, ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade union membership, genetic data, biometric data, and data on health, sex life and sexual orientation.

In this connection, it should be noted, as Mr Öman points out, that provisions relate to personal data that reveals one or more of the listed circumstances.[185] To deal with information that a person does not have a particular religious belief does not mean

[182] See Article 2 (d) Directive 2002/58/EC.
[183] See GDPR: EU Data Protection in the European Union, pages 100 – 101.
[184] Ibid., pages 100.
[185] See GDPR-En kommentar, page 244.

that it is revealed what religious beliefs he has because there are more than two, but I express this with caution.

The first exception, which allows the processing of sensitive personal data, is provided for in Article 9 (2) (a), which provides that such processing may take place after obtaining the consent of the data subject. The exception applies provided that a Member State has not transposed into national law a prohibition on the data subject being able to consent to the processing of sensitive personal data.

If the processing for the purpose of direct marketing includes sensitive personal data, a requirement for consent must be observed, which means that the legal basis of legitimate interest cannot support the processing of sensitive personal data. Theoretically, the processing of non-sensitive personal data could be based on legitimate interest, while the processing of sensitive personal data could be supported by consent. In my opinion, such an arrangement is not justified and would probably involve more work for the person responsible than benefit. When processing sensitive personal data, the processing is likely to depend on the sensitive personal data, and when consent is withdrawn, the processing is also likely to appear pointless. There is, therefore, no justification for the use of the legal basis of legitimate interest, but only consent should be used.

There should be an additional possibility, when exercising direct marketing, to process sensitive personal data on the basis of legitimate interest without obtaining consent. Such a possibility exists under Article 9 (2) (e) GDPR when the data subject has clearly made the sensitive personal data public. If the data subject makes such a disclosure, no consent is required for the processing of the published personal data. CJEU has ruled on the publication of personal data in a case from 2023.[186] As is apparent from that provision, there must be an unambiguous and active document on the part of the data subject.[187] It should be recalled that the exception provision be interpreted restrictively.[188] As regards information collected during a visit to a website, for example, by means of cookies, this constitutes information which, according to the CJEU, should not be construed as public.[189] Thus, the CJEU finds that information collected by cookies when a visitor interacts with a website does not constitute published information.[190] Such information that the data subject publishes on social media, for example, should not automatically be regarded as publicly made information. In line with the view of the CJEU, circumstances such as settings should be of importance in the interpretation of whether the data subject has made the information public. Publication is only likely to occur when the information is made available to an unlimited number of persons.[191] An assessment is thus required on a case-by-case basis in order to examine the data subject's choice of preferences regarding who has the opportunity to access his or her published information.[192] Finally, the data subject must make an informed disclosure, meaning

[186] See C-252/21, *Meta Platforms and Others (Conditions generaies dútilisation d'un réseau social).*
[187] Ibid., paragraph 77.
[188] Ibid., paragraph 76.
[189] Ibid., paragraph 78.
[190] Ibid., paragraph 84.
[191] Ibid., paragraph 82.
[192] Ibid., paragraphs 80 – 81.

that they must be aware that the published information is made available to an unlimited number of people.

Consequently, it should be possible, subject to certain challenges, to use the exemption for published information in the exercise of direct marketing, in which case sensitive personal data is processed. However, it may be difficult to rely on disclosure where personal data has been made available in forums other than social media, in which case consent must be obtained from the data subject.

5.7 A brief introduction to the Swedish Marketing Act´s significance in the question of consent

I would also like to mention in this context the importance of those who wish to engage in direct marketing looking beyond the provisions of the GDPR when choosing a legal basis. In order to highlight the need for compliance with national marketing law, I will briefly describe an essential provision in the Swedish Marketing Act, which I believe is of importance when an organisation is to choose a legal basis for its personal data processing.

Paragraph 19 of the Marketing Act[193] (MFL) prescribes how a marketer must behave when marketing its products or services to a natural person, when the marketing is carried out by electronic mail, fax, call machines or other similar automatic systems for individual communication that are not served by a human.[194] In such cases, Paragraph 19 of the MFL requires the prior consent of the natural person who is to receive the marketing.[195] In other words, according to a company, prior consent must be obtained in order to be able to send a newsletter (electronic mail) to a natural person. Marketing in which a natural person calls a potential customer is not covered by the provision, and for such a type of marketing, no consent is required.[196] In my opinion, this is a very strange way of dealing with the situation on the part of the legislator.

Anyone wishing to engage in direct marketing should, therefore, take into account whether national marketing law has provided for a special procedure. Where marketing law stipulates a requirement for consent, I find it inappropriate to use another legal basis to process personal data. Where another legal basis would be used, this means confusion and false expectations for the data subject who believes they can stop the processing by withdrawing their consent.

[193] Marknadsföringslag 2008:486, The Swedish Marketing Law.
[194] See Bernitz, Ulf. *Marknadsföringsrätten-Svensk och europeisk marknadsrätt 2.* 2th ed., Stockholm: Norstedts Juridik, 2020. [Cit: Marknadsföringsrätten, page 144.
[195] See Marknadsföringsrätten, page 145.
[196] Ibid., page 146.

5.8 Summary

Since the legal basis consent is not covered by the necessity requirement, non-necessary processing may be carried out by the controller. Thus, consent should be a very useful legal basis when the controller intends to engage in direct marketing. To the extent that the legal prerequisites described above are met, there is no need to examine whether the processing is necessary, which should make it easier for the controller. In addition, consent is very suitable as a legal basis for the exercise of direct marketing when the processing involves sensitive personal data, if cookies are used in the collection of personal data and where national marketing law requires consent. Since many circumstances may require consent in themselves, this constitutes a safe choice on which the controller can base their processing.

6 Summary and Conclusions

Finally, it can be stated that when a data controller, a non-public entity, wishes to engage in direct marketing, three of the six legal bases in Article 6 (1) of GDPR are relevant. The legal bases in question are consent, performance of a contract, and legitimate interest.

As regards the legal basis for the performance of a contract, I do not consider it appropriate to support the processing of personal data, where the controller is to carry out direct marketing. To use this legal basis, the processing must be necessary for the conclusion or performance of the contract, which must be interpreted strictly. It will likely be very difficult for the controller to demonstrate such a necessity. A contractual term meaning that the controller is allowed to process personal data to conduct direct marketing should be interpreted as consent incorporated in the agreement. Such baked-in consent usually does not meet the legal prerequisites for consent, which is why it is downright inappropriate to have such an arrangement.

On the other hand, a legal basis on which to base processing in the exercise of direct marketing is a legitimate interest. Direct marketing is a recognised legitimate interest by both courts and the EDPB. The decisive factor in the question of whether the processing is lawful and thus compliant with the GDPR depends on the balancing of interests that the personal data controller has to perform. In doing so, an overall assessment must be made of all the relevant circumstances of the processing, such as the legitimate interest, the reasonable expectations of the data subject, the potential and actual consequences for the data subject, and the necessity of the processing in relation to its purposes. It is, therefore, difficult, if not impossible, to establish a processing in the exercise of direct marketing as lawful in the exercise of direct marketing. This must be decided on a case-by-case basis. However, there is much to suggest that the commercial, legitimate interest weighs heavily in this context and, together with appropriate safeguards and the data subject's opportunity to opt-out, the balancing of interests should result in the personal data controller's favour.

The legal basis of consent is, in my view, the most appropriate basis of all of them for the exercise of direct marketing. On the basis of consent, the controller has the right to carry out even unnecessary processing of personal data, provided that the legal requirements for consent have been met. When personal data processing includes sensitive personal data or when Swedish marketing law is applicable, consent is required, which means that it is not sufficient in such a case to base the processing on legitimate interest. When cookies are used for marketing purposes in order to collect information and subsequently target marketing directly to the user, consent is required. That said, consent is not only the most appropriate ground; it is necessary to obtain it in some cases.

References

Official documents

European Union

Primary law

Treaty of the Functioning of the European Union and Treaty of the European Union. OJ C 202, 07.06.2016.

Charter of Fundamental Rights of the European Union. OJ C 326 26.10.2012.

Regulations

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

Directives

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (No longer in force)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification).

European Data Protection Board

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation. Version 3.0. 2019-06-04.

Guidelines 2/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. Version 2.0. 2019-06-04.

Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. 2020-05-04.

Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.1. 2021-07-07.

Article 29 Data Protection Working Party

WP 136. 01248/07/EN. *Opinion 4/2007 on the concept of personal data.* Adopted 2007-06-20.

WP 179. 0836-02/10/EN. *Opinion 8/2010 on applicable law.* Adopted 2010-12-16. (Updated thru WP 179 update. 176/16/EN. *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain.* Adopted 2015-12-16.)

WP 203. 00569/13/EN. *Opinion 03/2013 on purpose limitation.* Adopted 2013-04-02.

WP 217. 844/14/EN. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* Adopted 2014-04-09.

WP 259 rev.01. 17/EN. *Guidelines on consent under Regulation 2016/679.* Adopted 2017-11-28 and as last Revised and Adopted 2018-04.-10.

WP 260 rev.01. 17/EN. *Guidelines on transparency under Regulation 2016/679.* Adopted 2017-11-29 and as last Revised and Adopted 2018-04-11.

Sweden

Legislation

SFS 2008:486. *Marknadsföringslag.*

SFS 2018:218. *Lag med kompletterande bestämmelser till EU:s dataskyddsförordning.*

SFS 2022:482. *Lag om elektronisk kommunikation.*

Swesish Guvernement Bill

Prop. 2017/18:105. *Ny dataskyddslag.*

Swedish Guvernement Official Reports

SOU 1997:39. *Integritet ´Offentlighet´Informationsteknik.*

SOU 2015:61. *Ett stärkt konsumentskydd vid telefonförsäljning.*

Literature

Monographs

Bernitz, Ulf, Carlsson, Mia, Heuman, Lars, Leijonhufvud, Madeleine, Magnusson Sjöberg, Cecilia, Seipel, Peter, Warnling Conradson, Wiweka and Vogel, Hans-Heinrich. *Finna rätt – Juristens källmaterial och arbetsmetoder*. 15th ed., Stockholm: Norstedts Juridik, 2020.

Bernitz, Ulf. *Marknadsföringsrätten – Svensk och europeisk marknadsrätt 2*. 2th ed., Stockholm: Norstedts Juridik, 2020.

Hettne, Jörgen and Otken Eriksson, Ida (red.). *EU-rättslig metod – Teori och genomslag i svensk rättstillämpning*. 2th ed., Stockholm: Norstedts Juridik, 2011.

Kleineman, Jan. Rättsdogmatisk metod. *Juridisk Metodlära*. Nääv, Maria and Zamboni, Mauro (red.), 21 – 46. 2th ed., Lund: Studentlitteratur, 2021.

Krzysztofek, Mariusz. *GDPR: Personal Data Protection in the European Union.* 114th ed., Netherlands: Wolters Kluwers, 2021.

Kuner, Christopher, A. Bygrave, Lee and Docksey, Christopher. *The EU General Data Protection Regulation (GDPR) – A Commentary.* Oxford: Oxford University Press, 2020.

Öman, Sören. *GDPR (GDPR) m.m. – En kommentar.* 2th ed., Stockholm: Norstedts Juridik, 2021.

Articles

Michael Holtz, Hajo and Ledendal, Jonas. Överlappningen mellan dataskydd och marknadsrätt – GDPRs tillämpning på marknadsföring och marknadsrättens tillämpning på kommersiell personuppgiftsbehandling. *Svensk* Juristtidning. SvJT 2020 s. 143.

Case law

Court of Justice of the European Union

Judgement of 16 December 2008 in Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy,* ECLI:EU:C:2008:727.

Judgement of 16 December 2008 in Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, ECLI:EU:C:2008:724.

Judgement of 8 September 2011 in Joined Cases C-68/10 and C-58/10, *Monsanto SAS and Others v Ministre de l'Agriculture et de la Pêche,* ECLI:EU:C:2011:552.

Judgement of 25 October 2011 in Joined Cases C-509/09 and C-161/10, *eDate Advertising GmbH and Others v X and Société MGN LIMITED*, ECLI:EU:C:2011:685.

Judgement of 24 November 2011 in Joined Cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* ECLI:EU:C:2011:777.

Judgement of 13 May 2014 in Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

Opinion of 18 December 2014 in Case Opinion 2/13, *Opinion pursuant to Article 218(11) TFEU*, ECLI:EU:C:2014:2454.

Judgement of 19 October 2016 in Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

Judgement of 4 May 2017 in Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme",* ECLI:EU:C:2017:336.

Judgement of 20 December 2017 in Case C-434/16, *Peter Nowak v Data Protection Commissioner*, ECLI:EU:C:2017:994.

Judgement of 5 June 2018 in Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388.

Judgement of 29 July 2019 in Case C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV,* ECLI:EU:C:2019:629.

Judgement of 24 September 2019 in Case C-136/17, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL),* ECLI:EU:C:2019:773.

Judgement of 1 October 2019 in Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*, ECLI:EU:C:2019:801.

Judgement of 11 December 2019 in Case C-708/18, *TK v Asociaţia de Proprietari bloc M5A-ScaraA,* ECLI:EU:C:2019:1064.

Judgement of 17 June 2021 in Case C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited v Telenet BVBA,* ECLI:EU:C:2021:492.

Judgement of 15 July 2021 in Case C-60/20, *Latvijas dzelzceļš" VAS v Valsts dzelzceļa administrācija,* ECLI:EU:C:2021:610.

Judgement of 4 July 2023 in Case C-252/21, *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2023:537.

Judgement of 7 Mars 2024 in Case C-604/22, *IAB Europe*, ECLI:EU:C:2024:214.

Judgement of 7 Mars 2024 in Case C-479/22, *OC v Commission,* ECLI:EU:C:2024:215.

Supreme Administrative Court of Sweden

Judgement of 1 October 2001 in Case RÅ 2001 ref. 68, *Jordbruksverkets adressregister över mjölkproducenter har ansetts kunna lämnas ut för kommersiellt ändamål.*

Judgement of 24 June 2002 in Case RÅ 2002 ref. 54, *Utdrag ur Centrala studiestödsnämndens register över mottagare av studiemedel har ansetts kunna lämnas ut för kommersiellt ändamål.*

Judgement of 3 June 2016 in Case HFD 2016 ref. 40, *Personuppgiftslagens krav på att personuppgifter får behandlas bara om det är lagligt innebär att behandlingen ska vara förenlig med bestämmelserna i den lagen och i föreskrifter som har meddelats med stöd av lagen.*

Court of Appeal of Sweden

Judgement of 5 November 2020 in Case KRGBG 3486-20, *Rätt att ta del av allmän handling.*

Other Sources

Council of Europe. European Treaty Series no. 108. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Strasbourg 1981.

European Commission. Sweden and the Swedish membership. <https://sweden.representation.ec.europa.eu/om-oss/sverige-och-eu-medlemskapet_sv>(Accessed 2024-05-01).

European Convention on Human Rights.

Federation of European Direct and Interactive Marketing (FEDMA). *EUROPEAN CODE OF PRACTICE FOR THE USE OF PERSONAL DATA IN DIRECT MARKETING ELECTRONIC COMMUNICATIONS ANNEX.* Brussels. 2010.

International Chamber of Commerce (ICC). *ICC Advertising and Marketing Communication Code – Build consumer trust through responsible marketing.* 2018.

Integritetsskyddsmyndigheten. Intresseavvägning. 2021-09-15. <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/intresseavvagning/> (Accessed 2024-05-21).

Marshall, Ron. How Many Ads Do You See In One Day? *Red Crow Marketing INC.* 2015-09-10. <https://www.redcrowmarketing.com/blog/many-ads-see-one-day/> (Accessed 2024-05-20).