UiO : Faculty of Law
University of Oslo

The Balancing of Interests

A legal analysis of the balancing tests under Article 6 (1)(f) and Article 21 of the GDPR in relation to processing of personal data through video devices.

Candidate number: 9011

Submission deadline: 01 December 2021

Number of words: 15 004

Table of contents

1 INTRODUCTION 1

1.1 Background 1
1.2 Research Question, Challenges and Method 2
1.3 Structure of the Thesis 3

2 PROCESSING OF PERSONAL DATA THROUGH VIDEO DEVICES 3

2.1 Personal data or special categories of personal data? 6
2.1.1 Biometric data 7
2.2 Consent 9
2.2.1 Consent to processing of personal data through video devices 11
2.3 Summary 12
2.3.1 Recommendations 13

3 LEGITIMATE INTEREST, ARTICLE 6 (1) (F) 13

3.1 Purpose 15
3.2 Necessity 16
3.3 Balancing test 17
3.3.1 Impact on data subject 18
3.3.2 Balancing the rights 19
3.3.3 Safeguards 20
3.4 Summary 21
3.4.1 Recommendations 21

4 THE RIGHT TO OBJECT, ARTICLE 21 22

4.1 Where does the right to object not apply? 23
4.2 Where the right to object does apply 24
4.3 Balancing the interests 25
4.3.1 Reasons relating to his or her particular situation 25
4.3.2 Compelling legitimate grounds 27
4.3.3 Balancing the interests 28
4.4 Summary 29
4.4.1 Recommendations 30

5 CASE APPLICATION 31

5.1 Danish Football Stadium – facial recognition cameras by the entrance 31
5.2 Swedish Skellefteå High School – facial recognition based on consent 32

5.3 VoetbalTV – legitimate interest 34
5.4 Summary 36
5.4.1 Recommendations 36

6 CONCLUSION 37

TABLE OF REFERENCE 40

1 Introduction

1.1 Background

Within the past few years there has been an increase in the use of video monitoring and facial recognition video surveillance by public authorities. China has implemented its social credit system and the UK police department deploy facial recognition cameras for identifying criminals. Such processing is based on the arguments of public interest, national security, criminal proceedings etc, and is in accordance with the governments' approval. This invasion of privacy can arguably be justified, and numerous people may find it appropriate and proportionate. The use of video devices by public authorities are outside the scope of this thesis, nevertheless it valuable to understand that such processing is already in place. For private entities, on the other hand, the lawful ground for deploying video device cameras is more difficult to achieve.

While the processing of personal data through video surveillance is often justified by the public interest argument, such as security or prevention of crime, general processing of personal data through video device systems by private controllers cannot always be justified. There are several principles the controllers must take into account and adhere to when processing personal data; however, this paper will focus on the legal bases of processing under Article 6 (1) of the GDPR, more specifically the 'legitimate interest' basis, and the right to object to processing under Article 21 of the GDPR. Both the lawful ground of processing based on legitimate interest (Article 6 (1)(f)) and the right to object demand a careful assessment balancing the rights of the data subject and the interests of the controller. There is no specific answer to the balancing test, and every case must be decided on a case-by-case basis, and it is neither sufficient to refer to other cases. Accordingly, it can be difficult for data subjects and controllers to understand what may be lawful or not, unless the case subsequently is brought before the national data protection authority or court. In addition, the right to object was revised by the GDPR and is now providing an assumption in favour of the data subject.

Considering that new technology is developing quickly, paving the way for smart cameras, artificial intelligence and intelligent video analysis, this is certainly an area which is in tender need of regulation. The invasiveness such technology can have on individuals' right to privacy

and data protection is substantial, and with the GDPR which is fairly new, it can be difficult to understand how individuals' rights may be best protected. Although several cases concerning video surveillance have been brought to court for breach of the European Convention of Human Rights ("**ECHR**"), there are not so many cases concerning Article 6 and Article 21 of the GDPR. The lack of judicial precedence and the vague notion of 'balancing of interest' can make it difficult for private controllers and data subjects to understand their rights and interests.

For the purpose of this thesis, video device systems will include video surveillance, recordings, live-streaming, facial recognition cameras, videos uploaded to the internet and similar. This thesis is only concerned with the lawful bases for processing the data and the data subject's right not to be subjected to such processing. The main legislation to be addressed is the EU General Data Protection Regulation ("**GDPR**"), and primarily Article 6 (a), Article 6 (f) and Article 21.

1.2 Research Question, Challenges and Method

In light of the above concerns, this paper will assess and analyse the rights and interests of the controller and the data subject, and examine how this is applied in practice concerning processing of personal data through video devices. This paper will focus on the legal bases and the right to object under the GDPR, and only address processing of data conducted by private entities. The main research question will therefore be:

- To what extent does the balancing tests under Article 6 (1)(f) and Article 21 of the GDPR ensure an appropriate and proportionate balance between the data subject's rights and controller's interests?

In order to assess the main research question, this paper will examine how personal data can lawfully be processed through video device systems in four parts. It will first look at processing of personal data through video devices in general, followed by the legal bases for such processing. The third part will address the data subject's right to object, and lastly it will analyse how such processing is conducted in practice. In essence, the main research question can be divided into the following parts:

- A general overview of video recording systems, personal data and special categories of personal data, and the data subject's consent to processing.

- Does Article 6 (1) (f) ensure an appropriate balance of interests between the controller and the data subject?
- Does the right to object to processing under Article 21 provide an appropriate balance between the interests and rights of the controller and data subject?
- How is the legislation applied to processing of personal through vide devices in practice?

The number of private companies processing personal data by deploying video devices are still limited, however as a result of the developments in technology it is likely to increase. Furthermore, private companies already deploying video devices can often rely on the public interest as a lawful ground for processing. Private companies relying on legitimate interest is therefore not an area which has developed comprehensive precedence. In addition, there is limited discussion concerning the right to object in general. It is for these reasons that this thesis will attempt to address and analyse the application of the balancing tests following the legitimate interest ground and the right to object. There is limited judicial precedence and legal literature on the topic, hence this paper will adopt a legal research method focusing on legislation from the European Union, and the Article 29 Working Party's and European Data Protection Board's working documents.

1.3 Structure of the Thesis

This thesis is divided into four chapters. A general understanding of the processing of personal data though video devices, including the lawful basis of consent, is provided as a starting point. Chapter two will address the application of the lawful ground of processing based on 'legitimate interest', followed by an analysis of the balancing test. Chapter three will address the data subject's right to object to processing of personal data though video devices, focusing on the balancing of interests between the controller and the data subject. The last chapter will address three national cases within the EU and their application of the regulation concerning the processing of personal data through video devices, followed by some additional analysis. Some recommendations will be provided throughout the paper, in addition to a concluding remarks.

2 Processing of personal data through video devices

The European Convention on Human Rights ("**ECHR**") provides the framework for the protection of the vital rights and freedoms that all humans possess. Article 8 of the ECHR states that 'everyone has a right to respect for his private and family life'.[1] The right to protection of personal data is also established by the Charter of Fundamental Rights.[2] It demands that all personal data must be processed fairly, with a specific purpose and on the basis of consent received from the data subject or any other legitimate ground prescribed by law.[3] In addition, the GDPR, which came into force in 2018, provides the framework for the protection of personal data. The right to not be subject to processing of personal data though video devices has been established by multiple cases. In *Peck v. United Kingdom*[4] the ECtHR asserted that footage of the plaintiff which was submitted to the press and revealed the identity of the plaintiff constituted a breach of the Article 8 of the ECHR, and that the protection of such personal data was fundamental to the enjoyment of a persons' private life. In *Big Brother Watch & Others v. The United Kingdom*[5] the ECtHR ruled that the UK legislation enabling mass surveillance was in violation of human rights, and specifically the right to privacy under Article 8 ECHR.

The use of video devices has increased over the past few years in most parts of the world. Video devices may be utilized in both private and public places for a number of reasons. A private individual might wish to use video devices inside his or her house or on the property to prevent burglary or support the protection of the property, or use a video camera to record a cycling trip for his or her own use. A private company, on the other hand, might wish to use video surveillance cameras to prevent crimes, such as theft, increase the security or to deliver personalised advertisement. Despite what legitimate purpose one might have to make use of video devices, such technology could have an impact on people's behaviour and raise data protection concerns.[6] The knowledge of a CCTV camera watching will likely put pressure on individuals to prevent abnormal behaviour and limit the possibility of anonymous movement and use of services.

---

[1] European Convention on Human Rights, Article 8 (1)

[2] Charter of Fundamental Rights of the European Union (2000/C 364/01), Article 8

[3] Charter of Fundamental Rights of the European Union (2000/C 364/01), Article 8 (2)

[4] *Peck v. United Kingdom*, App No 44647/98, ECHR 2003-I, [2003] ECHR 44, (2003) 36 EHRR 41, (2003) 36 EHRR 719.

[5] *Big Brother Watch & Others v. The United Kingdom* (ECtHR, 13 September 2018) §387.

[6] EDPB 2019B: European Data Protection Board,'Guidelines 3/2019 on processing of personal data through video devices' (10 July 2019), p. 5

The different uses of video devices can be divided into three categories depending on which person or body who carries out the recording and for what purpose the footage is being made. Firstly, the use of video surveillance by competent authorities in order to prevent and investigate criminal offences and safeguarding public security are generally legal and are dealt with in the Law Enforcement Directive.[7] Such video surveillance is usually conducted in public spaces, especially where there is a heightened risk for crime, and there will often be a public interest in installing the cameras. Secondly, where the video recording is conducted in a purely personal or household activity, the recording can fall under the 'household exemption' and will be outside the scope of the GDPR.[8] The household exemption must be narrowly assessed, however, and what might seem to be video recording carried out in a private or family activity, may fall within the scope of the GDPR after all. For instance, a video recording which is published on the internet and made accessible to everyone will fall outside of the household exemption.[9] Furthermore, in relation to video surveillance systems which record and store personal data, if the camera even just partially covers a part of a public space, it will neither fall under the household exemption.[10]

The third and last category is where the use of video devices is conducted by a private person or entity where the processing of personal data falls under the GDPR. This can be where a sports club monitors the athletes of its team in order to better the performance of the whole team, or where a shop owner conduct video surveillance in order to enhance the security of the shop. In either case, personal data is being processed, and there are several matters to be considered when conducting such processing. It is this third and latter category that will be discussed for this thesis.

Development in technology has modified the traditional cameras to smart cameras, where the capturing of a picture can be used to uniquely identify people. Intelligent video analysis and use of artificial intelligence now allow video surveillance to be high performing, resulting in difficulties in preserving individuals' privacy.[11] Different techniques can be applied when

[7] Law Enforcement Directive (EU2016/680)

[8] GDPR, Article 2 (2) (c)

[9] European Court of Justice, Judgment in Case C-101/01, *Bodil Lindqvist case*, 6th November 2003, para 47

[10] European Court of Justice, Judgment in Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33.

[11] EDPB 2019B, Guidelines 3/2019 (10 July 2019, p.5

conducting CCTV, and the data privacy impact and application of law are dependent on what technique which is being applied.[12] The data privacy impact can usually be divided into two categories when concerning processing of personal data through video devices: less intrusive (personal data) and more intrusive (special categories of personal data).

Article 5 of the GDPR must be carefully considered when conducting video surveillance. Firstly, the processing of data must be conducted in a lawful, fair and transparent manner.[13] Where there is processing of personal data by video surveillance, the controller must give information about such processing, either by warning signs, in a written document or other methods. The processing must materialize for a specific and legitimate purpose, and the video data cannot be used for any other purposes or exceed the intended purpose.[14] The data should not be retained for a longer period than what is necessary to achieve the purpose,[15] and appropriate and technical measures must be put in place to secure and protect the data.[16]

2.1 Personal data or special categories of personal data?

Personal data or personal information is defined as any information relating to an identified or identifiable natural person.[17] To be a natural identifiable person it must be possible to identify the person, either directly or indirectly, through the personal information in question. Such information can be name, birth date, location data, phone number, email address or factors which can specify any 'physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[18] Under the GDPR it has been established a particularly stringent regulation of processing of special categories of personal data. Special categories of data is defined under the GDPR as any personal data '*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'*.[19]It is

[12] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.5
[13] GDPR, Article 5 (1) (a)
[14] GDPR, Article 5 (1) (b) and (c)
[15] GDPR, Article 5 (1) (e)
[16] GDPR, Article 5 (1) (f)
[17] GDPR, Article 4 (a)
[18] GDPR, Article 4 (a)
[19] GDPR, Article 9 (1)

not straightforward to determine whether the data falls under this category. The image of a person recorded by a camera generally falls under the definition of personal data.[20] The personal data does not necessarily have to be sensitive or intrusive on the data subject, nevertheless it is important to establish the gravity of intrusiveness. As a general rule of thumb, processing of data through video device systems will generally constitute processing of personal data or special categories of personal data. Extra care and caution must be performed where it is established that special categories of personal data are processed.

Video surveillance system collects and process massive amounts of personal data, and although the data can be highly personal and reveal unique identification of natural persons, it does not necessarily categorize as 'special categories of personal data'. If a video surveillance camera captures a woman in a wheelchair or a man wearing sunglasses, the video footage does not qualify as special categories of personal data.[21] If the massive amounts of video footage is used to map out a person's habits, however, then such data can constitute special categories of personal data.[22] For instance, video footage showing a person in a strike or taking part of different events can reveal the person's political opinions or religious believes, which would fall under the special categories of personal data under Article 9 (1).

2.1.1 Biometric data

Biometric data is personal data which reveals physical, physiological or behavioural characteristics. Unlike some personal data, like a name or email address, biometric data provide a unique identification of the natural person in question resulting specific technical processing.[23] As such, a video footage is not necessarily biometric data if it does not contribute to the identification of the data subject.[24] For the data to be biometric it must be processed for the purpose of uniquely identifying the data subject. For instance, a photograph is not biometric data unless it is processed through systematic technical means which allows for the unique

[20] Judgment of the CJEU, 11th December 2014, *František Ryneš v Úřad pro ochranu osobních údajů*, C-212/13, ECLI:EU:C:2014:2428, paragraph 22

[21] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 17

[22] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 17

[23] GDPR, Article 4 (14)

[24] GDPR, Recital 51

identification or authentication of the data subject.[25] Accordingly, to establish biometric data the data has to be: (a) data relating to physical, physiological or behavioural characteristics of a natural person, (b) data resulting from a specific technical processing, and (c) data must be used for the purpose of uniquely identifying a natural person.[26]

If it is established that the video surveillance system records biometric data and that that data is used by private companies for their own purposes, such as marketing or security, then an explicit consent from the data subject is required in nearly every case.[27] Explicit consent to processing of biometric data is not abnormal and it could materialize for the simplest of reasons. If a person unlocks his or her iPhone with FaceID or access his or her building through facial recognition, then an explicit consent would usually have been given priorly. When using facial recognition such as these, a biometric template would be generated after the data subject has made an explicit and informed consent.[28] For instance, data subjects must consent to using Apple's FaceID, and the iPhone will further take multiple photographs of the data subject's face from various angles in order to generate a biometric template. The biometric template will subsequently recognise the data subject (almost) every time the data subject attempts to unlock its iPhone, and it will in addition recognise who is not the data subject. Where biometric templates are generated, the controller must ensure that all intermediate templates are immediately deleted.[29] Intermediate templates are the footage taken in order to compare the data subject to the biometric template created by the data subject at the time of the consent.[30] In order to meet the purpose and necessity for processing, only the biometric template generated for the enlistment should be retained, and it must be retained exclusively for achieving the objective of the processing (e.g. unlocking the iPhone).[31]

Another issue arises where the controller cannot ensure that a data subject has given a prior consent. If there is a facial recognition method for entering a building, then the controller must have obtained explicit and informed consent from the data subject prior to the data subject's

[25] GDPR, Recital 51
[26] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 18
[27] GDPR Article 9 (2)(a) & EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 18
[28] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 19
[29] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 19
[30] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 19
[31] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 19

use of the access method. However, in order to not capture a footage of any individuals who have not consented, the facial recognition method for accessing the building should be triggered in some way, such as pushing a button or entering a code. The controller must always have another method for accessing the building, where there is no processing of biometric data, to ensure the lawfulness of the processing.[32] Similarly, a consent to processing of biometric data shall not be a condition for an individual's right to access a building or use of service.[33] The data subject must always be offered an alternative method, without additional cost, which does not involve biometric processing.

Where the video surveillance system does process special categories of personal data, the controller must identify an exemption for processing under Article 9 and a legal basis under Article 6.[34] Although all exceptions under Article 9 (2) can in principle be applicable, it is not likely that most of them are usable to justify the processing of special categories of personal data through video surveillance.[35] Article 9 (2) (e) which allows for processing of special categories of data which is made public by the data subject, is not an exemption to be relied upon by the mere fact that the data subject is walking in public or participated in a strike and was coincidentally caught by a video camera.[36] As previously mentioned, the most commonly used exemption is the 'explicit consent' under Article 9 (2)(a). In order for a controller to process personal data lawfully, it has to process the data based on one of the legal grounds prescribed in Article 6 (1) of the GDPR.[37] Processing of video surveillance data can in principle have a legal basis under every provision. In practise, however, the most common legal ground to be used are 'legitimate interest' and 'necessity to perform a task carried out in the public interest or in the exercise of official authority'.[38] In a few special cases the processing can also be based on consent.[39]

2.2 Consent

[32] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 19
[33] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 20
[34] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 17
[35] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 17
[36] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 17
[37] GDPR, Article 5 (1) (a)
[38] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 9
[39] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 18

Following Article 6 (1) (a) of the GDPR, personal information can be processed lawfully if the data subject has consented to the processing in a manner which satisfies the conditions for a valid consent. Firstly, the consent must meet the conditions specified in Article 7 GDPR. Where the request for consent is given in a written from, it must be presented in a way which clearly distinguish it from other matters.[40] The data subject should receive information concerning who the controller is, the purpose for which the personal data is processed and to what extent the consent is given.[41] The request shall be presented in an easily accessible form, where clear and plain language is used, making the request simple to understand for the data subject,[42] and it should not contain unfair terms.[43] If the processing of the data subject's personal data is conducted for multiple purposes, the data subject has to be informed of all the purposes and consent separately to each of them.[44] In addition, the data subject shall be informed of its right to withdraw the consent at any time, and the withdrawal shall be as easy to conduct as the affirmative action of consenting.[45]

Secondly, the consent must be freely given, specific, informed and unambiguous, and can be in the form of a statement or by a clear affirmative action.[46] Such consent can include a written or oral statement, 'ticking a box' (for example when consenting to cookies when visiting an internet website), choosing technical settings for social medias or by other affirmative actions clearly indicating the data subject's acceptance.[47] The requirement of an 'affirmative action' signifies that a consent cannot be given in silence or inactivity, such as by insinuating a consent because the data subject did not speak up or reject the processing. Furthermore, consent does not always provide the controller with legal ground for processing where there is a clear imbalance between the data subject and the controller, such as where the controller is a public authority.[48] The consent from the data subject should not be regarded as a valid legal ground if the data subject 'has no genuine or free choice or is unable to refuse or withdraw consent

[40] GDPR, Article 7 (2)
[41] GDPR, Recital 42
[42] GDPR, Article 7 (2)
[43] GDPR, Recital 42
[44] GDPR, Recital 32
[45] GDPR, Article 7 (3)
[46] GDPR, Article 4 (11)
[47] GDPR, Recital 32
[48] GDPR, Recital 43

without detriment'.[49] The burden of proof when demonstrating that a proper consent has been given lies with the controller.[50]

2.2.1 Consent to processing of personal data through video devices

If a person or entity are relying on consent for the processing of personal data resulting from video recording or surveillance, the consent must comply with the requirements of the GDPR as described above. It must be freely given, specific, informed and unambiguous.[51] Considering that a video surveillance system often captures footage of an unknown number of people before the data subjects can be informed of the monitoring, 'consent' can only in exceptional cases serve as a legal bases in accordance with Article 7 GDPR. In addition, it will be difficult for the controller to present evidence that the data subjects have consented prior to the processing of their personal data. Furthermore, if a data subject withdraws its consent, it will be complicated for the controller to evidence that the processing of personal data has discontinued.[52]

What constitute a freely given consent is another requirement which can be difficult to overcome. Video recordings of workouts and competitions are not unusual to athletes, and it is generally unproblematic to establish a valid consent where there is only one athlete being filmed for the athlete's purpose of enhancing its performance. On the other hand, if a theatre were to make video recordings of plays and make it available online for family and friends to watch, then it can be more problematic to establish a valid consent from each actor or actress. Most of the actors and actresses might be happy with having their play recorded, however there might be individuals that is declined to such processing. Nevertheless, individuals may feel pressured to consent so that their choices do not affect the others in the play.

There can neither be valid consent where there is a clear imbalance between the data subject and the controller,[53] thereby making it difficult for an employer to rely on 'consent' as a legal basis for conducting video surveillance of its employees. Given the clear imbalance between an employee and an employer, a consent will rarely be 'freely given'. An employer wishing to

[49] GDPR, Article 42
[50] GDPR, Article 7 (1)
[51] GDPR, Article 4 (11)
[52] GDPR, Article 7 (3)
[53] GDPR, Recital 43

process such data would generally have to rely on the legal basis of legitimate interest. A high school in Skellefteå in Sweden relied on 'consent' as a legal basis for running a pilot program which documented students' attendance through surveillance cameras with facial recognition.[54] The Swedish data protection authority assessed that the consent could not constitute a 'freely given' consent considering that the students were in a position of dependence of the school.

Where video recording is used to process special categories of personal data, the controller must find an exception under Article 9 (2) GDPR in order to process the data. Although all exceptions can in principle be applicable, the most common is to obtain explicit consent from the data subject.[55] As was recognised by the Swedish data protection authority in the Skellefteå case, the use of cameras with facial recognition constitutes the processing of biometric data which are extra worthy of protection and that explicit exceptions are required to conduct such processing. [56] Explicit consent is not defined by the GDPR, hence it may be difficult for controllers to establish if the consent it has received is explicit and valid. According to the UK data protection authority, the '**ICO**', an explicit consent is not likely to be very different from a general valid consent.[57] The main difference will presumably be that an explicit consent has to be made either orally or by writing, while a consent based on an affirmative action would not be explicit.

2.3 Summary

Personal data will be processed when deploying video devices in nearly every case. If the data which is being processed constitute special categories of data, then additional safeguards apply. The controller must in such scenario present an exemption under Article 9 (2). The additional safeguard serves as a proportionate measure considering that the data being processed is highly

[54] Datainspektionen, 'Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever'(20/08/2019) <https://www.imy.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf> (accessed 10th November 2021)

[55] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 18

[56] Datainspektionen, 'Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever'(20/08/2019) <https://www.imy.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf> (accessed 10th November 2021)

[57] Information Commissioner's Office, "What is valid consent?" < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what5> (accessed 12th November 2021)

sensitive. As a result, controllers cannot simply process personal data through facial recognition cameras where a lawful ground for processing has been established. It must, in addition, establish an exception.

Explicit consent is considered to be the most common exception to be applied under Article 9 (2), however the GDPR does not describe what constitute an 'explicit' consent. Presumably it is a consent which is stated either orally or by writing, and cannot be 'explicit' by a mere affirmative action. Nevertheless, considering that the ICO, which is a highly qualified organ, is not completely sure what an 'explicit' consent is, it is something that should be clarified. The stated consent must in addition meet the conditions for a valid consent. This can constitute a problem where employees or students, for example, wish to participate in a research program. Can there be a valid consent where there is a relationship of dependence between the data subject and the controller? It can be difficult to prove that the consent is freely given, thereby depriving the employees or students of the opportunity to participate in a program.

2.3.1 Recommendations

2.3.1.1 Defining 'explicit' consent

Considering that an 'explicit consent' is the most commonly used exception under Article 9 (2) and concern the processing of special categories of data, then a proper definition of what constitute 'explicit' consent should be accounted for. It is not sufficient that the ICO believes it is *likely* that it constitutes a consent made either orally or by writing. The European Data Protection Board, or any other competent body, should therefore produce a clarification of an 'explicit' consent.

3 Legitimate interest, Article 6 (1) (f)

Following Article 6 (1) (f) of the GDPR, personal data may be processed if it is necessary for the purpose of the legitimate interest pursued by the controller or by a third party to whom the data is disclosed. To establish a legitimate interest, it must be an interest which is recognised by Union or Member State laws, although it does not necessarily have to be explicitly

acknowledged.[58] A legitimate interest can, for instance, exist where there is an appropriate relationship between the controller and the data subject, such as where the data subject is a client, employee or in service of the controller.[59] Nevertheless, the data subject's reasonable awareness of the existence and extent of the processing of its data must be taken into consideration when establishing if such processing has a legitimate ground.[60] Other examples of legitimate interest are where processing is necessary to prevent fraud, or for direct marketing purposes.[61]

There is, however, an exception to 'processing on grounds for legitimate interest'. If the legitimate interest of the controller or the third party is overridden by the data subject's fundamental rights, freedoms and interests, then the grounds of legitimate interest will not be a legal basis for processing.[62] When assessing the data subject's rights, one must take the reasonable expectations of the data subject, based on its relationship with the controller, into account.[63] For instance, if the data subject does not reasonably expect further processing, then the data subject's rights might override the controller's.[64] In addition, the nature and sensitivity of the processing must be considered, including the impact such processing can have on the data subject. Additional account must be taken if the data subject is a child (generally under 16-years-old[65]).[66]

In *Rīgas satiksme* it was established that there are three criteria that have to be assessed in order to establish a legitimate interest for the processing of video surveillance data: (a) A legitimate interest have to exist, (b) the processing is necessary to achieve the controller's purpose, and (c) balancing the interests.[67]

---

[58] Kuner, Christopher, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler, eds. *The EU General Data Protection Regulation (GDPR): A Commentary*. New York: Oxford University Press, 2020. Oxford Scholarship Online, 2021. ('Kuner, Bygrave, Docksey, Drechsler, 'GDPR: A Commentary'), p. 337

[59] GDPR, Recital 47

[60] GDPR, Recital 47

[61] GDPR, Recital 47

[62] GDPR, Article 6 (f)

[63] GDPR, Recital 47

[64] GDPR, Recital 47

[65] See GDPR, Article 8 (1), paragraph 2, which states that Member States can lower the age of what constitutes a child, however the age cannot be below 13 years.

[66] GDPR, Article 8

[67] Judgment of the ECHR, 4th May 2017, *Rīgas satiksme*, Case C-13/16

3.1 Purpose

According to the Article 29 Working Party ("**WP29**")[68] the 'notion of a legitimate interest could include a broad range of interest, whether trivial or very compelling, straightforward or more controversial'.[69] Although the list is non-exhaustive, the WP29 has listed several common contexts where the legitimate interest issue has arisen. Such interests include where the processing is based on the purpose of: freedom of expression; direct marketing; enforcement of legal claims; prevention of crime; security; employee monitoring for safety or management purposes; historical, scientific or statistical purposes; and research.[70] The interest pursued must be in accordance with Union or Member State laws, be sufficiently clear to allow the balancing test, and represent a real and present interest.[71]

The processing of video surveillance data can be lawful if it is necessary to achieve a purpose of a legitimate interest of the controller. The legitimate interest can be based on a legal, economic or non-material purpose, and it must be of a present issue.[72] A video surveillance camera cannot simply be installed if there is no purpose materialising from a situation of distress.[73] For instance, an employer who installs video surveillance cameras for the purpose of mapping out who has the longest lunch break or goes home early will not likely have a legitimate interest. If an employer suspects that one of the employees are stealing, on the other hand, then the processing could be legitimate for the purpose of revealing what employee who is stealing. Reports of former incidents, such as theft, assault or vandalism, can be strong arguments in establishing a legitimate interest for processing of data though video devices.

[68] WP29, which is the predecessor of the European Data Protection Board

[69] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217 (9 April 2014), p. 24

[70] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217 (9 April 2014), p. 25

[71] Ibid, Article 29 Data Protection Working Party, Opinion 06/2014, p. 25

[72] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.10

[73] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.10

Mere commercial interest will generally not be enough for establishing a 'legitimate interest'.[74] In *Google Spain* it was expressed that where there is a potentially serious interference of privacy and data protection, "it is clear that it (the processing) cannot be justified by merely the economic interest' of the controller".[75] The interests can, however, be partly based on commercial interest, in addition to other interests, which may justify serious interference with the data subject's privacy. Furthermore, the legitimate interest of third parties could potentially have an effect on the interest of processing along with the controller's interests.[76] The data subject's protected rights and interests[77] will in general override the interests of other third parties, however the balance between the interests may depend on the nature of the information and its sensitivity for the data subject.[78] In *TK v Asociaţia de Proprietari bloc M5A-ScaraA* it was empathised that the data subject's rights and freedoms should be balanced against all the third parties' interests.[79] The case concerned an apartment building which installed video surveillance cameras at the request of co-owners of the building. The plaintiff owned an apartment in the building and claimed that the video surveillance was conducted unlawfully. According to the court, the plaintiff's rights and freedoms had to be balanced against the interests of all the other co-owners of the building.

3.2 Necessity

The processing of data must be 'adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed'.[80] Accordingly, the processing of personal data must be targeted and proportionate in order to achieve the purpose of the controller.[81]

---

[74] Kuner, Christopher, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler, eds. *The EU General Data Protection Regulation (GDPR): A Commentary*. New York: Oxford University Press, 2020. Oxford Scholarship Online, 2021. ('Kuner, Bygrave, Docksey, Drechsler, 'GDPR: A Commentary'), p.337

[75] Judgment of the CJEU, 13 May 2014, *Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, no. C-131/12, ECLI:EU:C:2014:317 ('*Google Spain*'), paragraph 81

[76] *Google Spain*, paragraph 81

[77] European Charter of Fundamental Rights, Article 7 and 8.

[78] *Google Spain*, paragraph 81

[79] Judgment of the CJEU, 11th of December 2019, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 59

[80] GDPR, Article 5 (1) (c)

[81] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.82

Considerations should be made concerning if it is reasonable to conduct such processing, or if there is another less intrusive way to achieve that purpose.[82]

In relation to this, processing of video surveillance data should be avoided if there are other methods for achieving the purpose which are less intrusive to the fundamental rights of the data subject. Such methods can be hiring security personnel, fencing the property, or installing security locks and alarms. The use of video surveillance can also differ depending on the purpose to achieve. In some cases, the purpose can be achieved with real-time monitoring without storing the data, where for example a person watches the live recording for security measures. In other cases, the purpose might only be achieved where the data is stored. In such cases the video surveillance data might only be used where a crime or incident have happened, and it should not be stored for a longer period than what is necessary to achieve the purpose for processing. It is here worth to consider the invasiveness such surveillance can have on individuals. Is it better to have an employee always watching the real-time monitoring, or to have an employee only watching the video footage after a crime has happened? The controller should always have the purpose for processing in mind when establishing the method for video surveillance.[83]

Considering the nature of video devices' invasiveness, the controller should always limit the processing of personal data to what is necessary to achieve its purpose. If the purpose is to protect a controller's premises, then it will not be necessary to have video cameras installed outside the property boundaries.[84] If the purpose is to protect the property's garden from vandalism, the cameras should not even partially cover the public space outside the property, such as the streets. The controller must always assess where and when it is strictly necessary to operate a camera device system.[85]

3.3 Balancing test

When establishing if the controller can base the processing on the legitimate interest ground, the controller must perform a balancing test by taking the principle of proportionality into

[82] Ibid, ICO, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.84
[83] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.11
[84] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.11
[85] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p. 10

account.[86] The balancing test is mandatory, and it has to be evaluated carefully.[87] The test requires a careful assessment of the context and circumstances of which the processing of personal data is conducted, including the controller's interests and the potential interference with the data subject's rights and freedoms. According to the WP29, the balancing test must be a genuine one, and it should neither weigh in favour of the data subject or the controller.[88] The term 'genuine' should be understood as an fair and reasonable assessment where there is no partiality to either side.[89] Such cases must be assessed on a case-by-case basis in order to demonstrate whether the controller's interests override those of the data subject.[90] The interests of the controller can range from insignificant to compelling, and vice versa for the data subject, hence the balancing of interests might not always be so easy to assess. As a starting point, however, there are four general assessments to be conducted when carrying out the balancing test: (a) assessing the controller's legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.[91]

3.3.1 Impact on data subject

When assessing the impact processing of data will have on the data subject, the controller must consider to what extent the processing affects the data subjects' rights and freedoms, and if the processing will cause any negative impact or consequences on the data subjects' rights.[92] The intensity of intrusion for the rights of the data subject will vary depending on the type of information which is being processed, the number of data subjects being processed, the scope of processing and the circumstances of processing.[93] Account must be taken of the nature of the

[86] Kuner, Bygrave, Docksey, Drechsler, 'GDPR: A Commentary', p. 338

[87] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.11

[88] Article 29 Working Party, Overview of results of public consultation on Opinion on legitimate interests of the data controller (Opinion 06/2014), p.3

[89] Ibid, Article 29 Working Party, Overview (Opinion 06/2014), p.3

[90] Ibid, Article 29 Working Party, Overview (Opinion 06/2014), p.3

[91] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217 (9 April 2014), p.33

[92] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.11

[93] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.12

processing, such as how sensitive the data is, the method of processing and the number of people having access to the data.[94]

The data subject's reasonable expectations concerning the context and circumstances of processing must also be assessed. Although one could assess the data subject's subjective reasonable expectation, the criterion is rather to determine what an objective third party could reasonably expect.[95] There are certain areas where objective individuals would generally not expect to be subject to processing of personal data through video devices. In addition, the relationship between the controller and a data subject may affect the expectation of processing personal data. A student would not reasonably expect to be monitored at school, or an employee would not reasonably expect to be monitored at its workplace. Similarly, bathrooms, saunas, restaurants, private homes, sitting areas and restaurants are neither places where an objective data subject would expect to be monitored by a video device. On the other hand, an objective person could expect there to be video surveillance at certain museums, banks or police stations.

3.3.2 Balancing the rights

The balancing of interests has to be decided on a case-by-case basis. Considering that every case is different and the invasiveness of privacy may vary, the balancing test is an important tool in order to appreciate all interests at stake. It is not sufficient to reference abstract situations or refer to other cases.[96] Where there are several data subjects, the interests of the data subjects as a group must be taken into account.[97] Sometimes the balancing test will be easier to assess. For instance, where a private car park is experiencing theft and vandalism and wish to deploy video surveillance at night in order to prevent crime, most individuals utilizing the car park would possibly appreciate the surveillance. Similarly, many individuals might feel safer in areas with more crime if video surveillance is conducted.

To what extent is the controller's legitimate interests trivial enough to overcome the rights and freedoms of the data subject? The interests of health, safety and security are likely to be trivial

[94] Judgment of the CJEU, 11th of December 2019, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 57

[95] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.12

[96] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.12

[97] EDPB 2019B, Guidelines 3/2019 (10 July 2019), p.12

enough for processing though video devices. Nevertheless, if the controller wishes to implement facial recognition cameras for security reasons, would that measure be too invasive on the data subject? Pharmacies in central cities are can potentially be visited by drug abusers, which neither employees or objective costumers will always find to be pleasant. If a pharmacy were thereby to implement facial recognition cameras in order to identify the regular drug addicts for security purposes, it may potentially have a recognised interest.[98] On the other hand, there is little information on how trivial an interest is where the interest is based on amusement, enjoyment or for delivering a helpful tool. In addition, balancing the interests can prove to be difficult where the data subject's interests are apparent, although not so compelling that it without question would override the interest of the controller. The many factors surrounding the processing of personal data through video devices must be subject to careful considerations, and the balancing test oblige the controllers to assess all of those factors. It can therefore be assumed that the balancing test serve as a helpful tool for the controller in order to make a proportionate assessment of the rights and interests between the controller and the data subject.

Nevertheless, the test can potentially be defeated by human errors. Everyone is different, and what may be important to the data subject, might be irrelevant for the controller. Considering that it is up for the controller to address the balancing test, it could potentially be demanding to conduct an objective test. As a result, the balancing test might rarely be an objective assessment.

3.3.3 Safeguards

Although the data subject's rights might way heavier than that of the controller, the safeguards the controller implement can tip the scale in the controller's favour. If safeguards are implemented in order to reduce the impact on the data subject, and those safeguards are adequate and sufficient, then the data subject's rights may be overridden.[99] Strict limitations of the collection of data, anonymisation of data, immediate deletion of data and opting out possibilities are means that can be put in place in order to safeguard the personal data processed. This does not imply that safeguards alone can justify the processing, nevertheless it can be used

[98] Although it also needs to find an exception under Article 9 (2) GDPR

[99] Article 29 Data Protection Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", 844/14/EN WP 217 (9 April 2014), p.31

as an important tool in order to limit the risk of the processing of the personal data, thereby reducing the data subject's privacy interference and data protection.

3.4 Summary

The criteria for establishing a legitimate interest is straightforward in the sense that there is a specific "checklist" the controller must follow. It must first establish a purpose, followed by assessing if the processing is necessary for achieving that purpose. If the controller is satisfied that the two requirements are met, then it can proceed to the balancing test. When conducting the balancing test, the controller must consider its own interests in processing the personal data and the impact the processing can have on the objective data subject. Appropriate safeguards implemented by the controller should also be considered.

The balancing test compliments the legitimate interest ground for processing in the sense that it attempts to preserve and value the different interests at stake by considering different factors. By employing the controller to carefully assess all the factors, a legitimate ground can be established by discretion. A descriptive and comprehensive legislation would not be able to make a justified decision where all the interests at stake, safeguards and necessity of each individual case are considered. Balancing the interests of the controller and the data subject's rights and freedoms is not straightforward, however, and can be an obstacle for the controller when establishing a legitimate interest. As there is no specific list containing all legitimate interests a controller may have, including if the interests are trivial or non-essential, it may be difficult for the controller to comprehend the gravity of its interests. Furthermore, it may be complicated for the controller to achieve an objective assessment of the balancing test, regardless of whether its intentions are pure.

3.4.1 Recommendations

The balancing test does to some extent ensure an appropriate and proportionate balance between the rights and interests of the data subject and the controller. Considering all the factors to take into account and that all cases must be assessed on a case-by-case basis, there might not exist a measure for ensuring a complete and absolute test establishing a justifiable and legitimate decision in every case. Regardless, the following recommendations can accommodate in creating more harmonized and predictable rules for establishing a legitimate interest.

3.4.1.1 A 'legitimate interest list'

The European Data Protection Board ("**EDPB**") could produce a 'legitimate interest' list that contain many relevant interests, and rate the different interests after value and importance. Is the interest trivial and significant? Or is it non-essential and meaningless? Although it is not sufficient to refer to other cases, which thereby presumably can also be applied to this 'list', it would give controllers an indication of how trivial or non-essential their interests are. The list should also contain third parties' interests and how much they could influence the overall 'legitimate interest'. Could the third party interests of enjoyment, for example, be of value to the balancing test?

3.4.1.2 Establishing clear boundaries

Another measure that could be implemented is by establishing clear boundaries of where processing through video devices is allowed and where it is not allowed. Considering that the notion of legitimate interest is non-exhaustive, compared with the invasiveness of processing of data through video devices, it might be appropriate to establish some areas where processing of personal data through video devices may be suitable or not.

3.4.1.3 Additional safeguards

The processing of personal data through video devices is, as discussed, intrusive on the data subject, hence it might be appropriate to develop additional safeguards for the data subject. The increase in technological developments will likely expand the use of video devices, and such expansion should be recognised in the balancing test. In that regard it can be considered if the balancing test concerning the processing of personal data through video devices should be reversed, making the controller liable to establish if its legitimate interest override that of the data subject.

4 The right to object, Article 21

"The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1), including profiling based on those provisions."[100]

The data subject has in some circumstances the right to object to the processing of its personal information relating to his or her particular situation.[101] The effect of an objection is that the controller must stop processing the personal information it collects, in addition to erasing the personal data it has already collected.[102] The right to object is subject to some conditions, however, where the lawfulness of the processing must be considered.[103]

4.1 Where does the right to object not apply?

The right to object does not apply if the lawfulness of processing is based on Article 6 (a)-(d) of the GDPR, however there are other alternatives to stop the processing. Where the processing is based on the data subject's consent,[104] the data subject can object to processing by way of withdrawing its consent.[105] This can, as an example, be when consenting to share your phone contacts with a social media in order to find new friends on said media. Furthermore, if the processing of personal data is based on a contractual relationship,[106] where the processing is necessary to perform a contract, then an objection would generally be performed by terminating the contract. For instance, a travel agency would not be able to fulfil its contractual obligations towards a person if the person objected to having its name and contact details processed, and as such, the contract would have to be terminated. In addition, where processing is necessary to comply with the controller's legal obligations,[107] or in order to protect vital interests of the data subject or others,[108] then the controller will not be under an obligation to comply with an objection to processing.

[100] GDPR, Article 6 (1)
[101] GDPR, Recital 69
[102] GDPR, Article 17 (1) (c)
[103] GDPR, Article 6
[104] GDPR, Article 6 (a)
[105] GDPR, Article 7 (3)
[106] GDPR, Article 6 (b)
[107] GDPR, Article 6 (c)
[108] GDPR, Article 6 (d)

4.2 Where the right to object does apply

The right to object applies to three circumstances of processing. An absolute right to object, with no exceptions, is where the processing of personal information in conducted for direct marketing purposes.[109] In such circumstances, the controller must stop processing the personal data without undue delay. When the processing of personal data is conducted in order to perform a task in the public interest, or when the controller is exercising a task as an official authority, the data subject has the right to object to the processing of its data.[110] Similarly, a data subject can object if the processing of its data is based on the legitimate interest of the controller or a third party.[111] However, the controller does not have to comply with the objection if it can demonstrate 'compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject', or where processing is necessary in order to comply with a legal claim.[112] Following Recital 69 of the GDPR, the data subject's objection must be based on his or her particular situation. The lawfulness of processing will further be determined by balancing the individual's particular situation against the controller's legitimate interest.[113] The responsibility of proving that the legitimate interest overrides that of the data subject lies with the controller.[114]

A balancing test between the rights and interests of the data subject and controller has already been assessed where the processing is based on the legitimate interest ground. Although the controller may find that it has a legitimate ground for processing which overrides the rights and freedoms of the objective and reasonable data subject, the right to object enables the particular situation and circumstances of the specific data subject to be taken into account.[115] As empathised by the WP29, the right to object does not contradict the balancing test in Article 6 (f), "it rather complements the balance, in the sense that, where the processing is allowed further to a reasonable and objective assessment of the different rights and interests at stake, the data subject still has an additional possibility to object on grounds relating to his/her particular

[109] GDPR, Article 21 (2)(3)
[110] GDPR, Article 21 (1)
[111] GDPR, Article 21 (1)
[112] GDPR, Article 21 (1)
[113] European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)' (7th July 2020), p.9
[114] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.141
[115] *Google Spain*, paragraph 76

situation."[116] The controller must subsequently conduct a new assessment of the balancing test. Where there is a public interest, such interest must be balanced against the data subject's rights and freedoms while taking the data subject's particular situation into account. The data subject may address the objection directly to the controller, who must subsequently examine if the processing of data can still be justified.[117] Where the controller does not comply with the request, the data subject may lodge a complaint towards the Data Protection Authority in his or her jurisdiction.[118]

4.3 Balancing the interests

Under the Data Protection Directive (1995), it was for the data subject to demonstrate that it had 'compelling legitimate grounds relating to his (or her) particular situation' in order to oppose processing of its personal data.[119] The GDPR does, however, provide an assumption in favour of the data subject by shifting the burden of proof by employing the controller to demonstrate that its compelling legitimate interest overrides that of the data subject. The right to object under Article 21 GDPR applies to video surveillance where the processing is based on a legitimate interest or for the necessity of carrying out a task in the public interest. The data subject can object on grounds relating to his or her particular situation, and the data controller can continue processing if it has compelling legitimate grounds which override that of the data subject. The data controller is obligated to respond to the request with undue delay, or at least within one month.[120]

4.3.1 Reasons relating to his or her particular situation

If an individual wishes to exercise its right to object, it must provide a specific reason for why it wants the controller to stop processing his or her personal information.[121] This specific reason must be based on the individual's particular situation.[122] A 'particular situation' is not defined

[116] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217 (9 April 2014),

[117] *Google Spain*, paragraph 77

[118] *Google Spain*, paragraph 77

[119] DPD (1995), Article 14 (a)

[120] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.144

[121] Ibid, ICO, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.140

[122] Ibid, ICO, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.140

in the GDPR, thus in some circumstances it might be difficult for the controller to determine the gravity of the data subject's situation. It can be obvious, such as where a person with a handicap object to be featured in a school campaign, or where the processing is causing the individual substantial damage, distress or financial loss.[123] For instance, a 15-year-old boy in a wheelchair may have a stronger and more apparent interest in not being recorded by a video camera, than a 25-year-old person with stage fright. On the other hand, should the latter person's objection be rejected just because stage fright is not serious enough? Establishing the gravity of an individual's particular situation will depend on each individual, the circumstances of processing and the nature of processing. Each case is different, and each individual can potentially have a particular situation even though the 'situation' is not visible or apparent. According to the EDPB, a 'particular situation' can also include information which constitutes slander, hate speech, factual inaccuracy or invasion of privacy.[124]

On the other hand, where the objection is manifestly unfounded or excessive, the controller can refuse to comply with the objection.[125] According to the ICO, an objection request may be excessive or unfounded where it is repetitive, overlaps other requests, is malicious or similar.[126] An individual who makes a request in order to harass an organisation, with the purpose of causing disruption or ruin for other data subjects, would submit an unfounded objective. Other unfounded examples are when the objection is based on the purpose of targeting someone, where there are unsubstantiated accusations or where the individual clearly has no intention of exercising the right. Considering that the controller must be able to demonstrate why it has rejected a data subject's objection, it may be difficult to ascertain if the objection is excessive or manifestly unfounded. The request must be considered in the context in which it was submitted, and it should be clear and obvious that the objection was unfounded. According to the ICO, the controller can even request a reasonable fee from the data subject if it is satisfied that the objection is manifestly unfounded or excessive.[127]

[123] Ibid, ICO, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.141

[124] European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)' (7th July 2020), p.9

[125] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.143

[126] Ibid, ICO, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.143

[127] Ibid, ICO, "Guide to the General Data Protection Regulation (GDPR)" (2018), p.143

The obligation to respond the data subject at the latest within one month is an obligation which does not necessarily serve the data subject's right. Where a high school play is recorded and uploaded to the internet for others to watch, and a person from the play objects to such recording afterwards, the controller of the video does not have to comply until one month later. In such a scenario, the video recording could stay online without the data subject's acceptance for one whole month. By that time, the video recording would probably have met its purpose and most parties interested would have seen the footage.

4.3.2 Compelling legitimate grounds

It is not established what constitutes 'a compelling legitimate ground for processing which overrides the interests, rights and freedoms of the data subject', and this is seemingly an issue which must be decided on a case-to-case basis. When deciding whether its legitimate interest overrides that of the data subject, the controller must ascertain the legitimate ground its processing is based on and assess if the reason for processing is compelling enough to justify further processing. Security reasons, criminal investigations or safety reasons are generally interests which will override the rights, interests and freedoms of the data subject. If the controller's interest is based on the enjoyment of others, or as a supportive tool for others, then the interest might not be so compelling.

When establishing a lawful ground under 'legitimate interest',[128] third party interests will also be taken into account. It is unclear if the same applies to the balancing test for a right to object. Article 21 (1) GDPR states that the controller must demonstrate compelling legitimate grounds, with no mention of whose legitimate ground. It therefore could seem that Article 21 (1) provides some leeway in the sense that it does not only have to be the controller's legitimate interest, but that it can also be that of others. Video cameras monitoring multiple spaces inside a concert stadium to prevent crowd surges and harm to the audience may be in the interest of the audience. One could assume that such third party interest could be taken into account when establishing a compelling legitimate interest which overrides the rights and freedoms of the data subject. On the other hand, Recital 69 of the GDPR states that the controller must demonstrate that *its* compelling legitimate ground overrides that of the data subject. It is therefore uncertain whether the balancing test should include the interests of third parties, be based on the legitimate ground

[128] GDPR, Article 6 (1)(f)

which the controller established as a lawful ground for processing, or if it is only the controller's legitimate interest which should be assessed.

Whether the interests of third parties are included in the balancing test or not is debatable. In the circumstances surrounding the use of video devices it is common that multiple people are caught on the footage. One objection thus has the capacity to destroy many others' enjoyment of the video devices. Suppose a football team wishes to film its football match in order to show it to family and friends, and one player object to the footage, then the rest of the team's players would be deprived of their enjoyment of the video footage. Third party's enjoyment or appreciation is not, however, an interest which is explicitly recognised as compelling. If the third party's interest had been relating to security or prevention of crime, then it is likely to be legitimate.

4.3.3 Balancing the interests

Similarly to the balancing test when establishing 'legitimate interest', what constitute 'a compelling legitimate ground' or 'particular situation' must be assessed on a case-by-case basis and will depend on the individual who assess the test. A sports enthusiast may be of the opinion that everything relating to sports will override individuals' rights and freedoms, while a digital rights advocate may believe that nothing is more important than a person's right to privacy and data protection. In addition, the arguments stemming from the data subject or the controller may range from very persuasive to very unconvincing, resulting in a balancing test which could be difficult to assess.

Considering that the test is to establish a compelling legitimate ground which overrides the rights, freedoms and interests of the data subject, the assumption is in favour of the data subject. There is little guidance on how to approach the right to object, including proper definitions of 'compelling legitimate ground' and 'particular situations'. How can the gravity of a 'particular situation' be determined? The situation can be apparent, such as physical, but it can also be psychological. It is difficult to assess if a data subject with severe social anxiety is lying, and it would be inappropriate to ask for any documentation of such. In addition, an individual with a 'particular situation' might not wish to come forward with his or her situation. Another issue is the gravity of the particular situation. Is it enough to establish that the data subject is shy or does not like to be photographed? Considering the invasiveness of a video camera, the threshold

for an objection should be lower than in most other situations of processing, or maybe there should be no threshold at all.

Furthermore, what constitute a legitimate interest which override the particular situation of the data subject? As discussed, a legitimate interest can range from uncompelling to very compelling, however it is not clear where the interest overrides the data subject's rights, freedoms and particular situation. One can assume that such interest include prevention of crime, security and health, and similar. Nevertheless, without clear definitions and guidance, it could prove difficult for a controller to assess if it has such a compelling legitimate ground and can continue processing of the personal data. Without the proper guidance for the balancing test, it is unclear if the legitimate interest even has to be very compelling. In addition, it will be difficult for the controller to conduct an objective assessment, especially without proper definitions and guidance. Arguably, the balancing test should be left to a third party with no connection to either the controller's interest or the data subject. In such a scenario, the balancing test would be conducted in an objective manner.

4.4 Summary

The data subject's right to object complements the balancing test of rights and interests in the sense that where processing is allowed, the data subject still has an additional possibility to object on grounds relating to his or her particular situation. The controller must subsequently establish compelling legitimate interest which overrides that of the data subject in order to continue the processing of data.

There are, however, multiple weaknesses stemming from the vague definitions and guidance for the balancing test. What is a 'particular situation' or a 'compelling legitimate ground'? How compelling must the controller's interest be in order to override the rights and freedoms of the data subject? Can third party interests influence the balancing test? Without proper guidance to answer these questions, it can be difficult for the controller to conduct an appropriate and proportionate balancing test. The pitfall for the controller is that without any proper guidance and straightforward legislation, it may have to reject the objection and await a possible interference by the national data protection authority, in order to truly know if its further processing is justified or not. It is therefore paramount that such guidance and regulation is put

in place to ensure that all private actors handle the personal data they process carefully and in accordance with applicable law. Three recommended measures are therefore proposed:

4.4.1 Recommendations

4.4.1.1 Guidelines

At the time being it seems rather unclear how private entities should respond to an objection. It is therefore preferable to establish clear guidelines for how to approach the balancing test when an objection is submitted. Although the balancing test is of value considering that every case is different, there should be established some straightforward and comprehensive guidance on where an objection is justified and where it is not. For instance, there could be clear boundaries for where an objection should be allowed in any case, despite how 'particular' the data subject's situation is. In addition, the guidelines should include the threshold for a 'particular situation'. How severe should the situation of the data subject be, or is it sufficient that the data subject is shy? On the other hand, considering the invasiveness of video cameras in general, maybe the threshold for a 'particular situation' should be removed completely.

4.4.1.2 Establish clear definitions

The legislation and guidance on the right to object does not properly address what constitute a 'compelling legitimate ground' or a 'particular situation'. Without proper definitions, it will be difficult for a controller to assess the balancing test or for the data subject to know its rights. Establishing clear definitions for what constitute a 'particular situation' and a 'compelling legitimate ground' is therefore of utmost importance in order to ensure that the balancing test can be carried out in a justified and proportionate manner. In addition, it must also be clarified whether third party interests are included, and to what extent they are influencing the balancing test.

4.4.1.3 Data Protection Authorities

In some Member States, private entities actively seek advice and approval from the data protection authority before the processing of personal data emerge. The data protection authorities can serve as an objective third party, and is thus capable of making objective

decisions while taking into account both the controller's interests and the data subject's particular situation. It may therefore be recommended that data protection authorities should receive special guidance on how to approach the balancing test, and that they should account for all the decisions concerning the right to object. This option may serve as helpful tool for controllers as well, considering that a justified decision is reached and that they can avoid a possible interference by the data protection authorities at a later point.

5 Case Application

5.1 Danish Football Stadium – facial recognition cameras by the entrance

After the discussion above, one could assume that the processing of special categories of data through video devices by private entities would be under strict regulation, and that it could only be justified in very special cases. Regardless, the Danish Data Protection Authority has approved the use of facial recognition cameras by the entrance of a football stadium run by a private entity.[129] The cameras are used to identify individuals who are banned from the stadium, and in order to achieve that purpose it will also capture footage of every other spectator in the process. The processing is based on Article 9 (2)(g) of GDPR which states that special categories of data can be processed if necessary for reasons of substantial public interest. The processing is also in accordance with the Danish Data Protection Act (2018) §7(4).[130] The football club has put in place measures and safeguards to comply with the GDPR by notifying the spectators entering the stadium, deleting the data at the end of the day and insulating the system from the internet.[131] Nevertheless, the measures of deploying facial recognition cameras have been subject to criticism from digital rights advocates concerning the invasiveness and impact it will have on individuals.[132] Is the public interest so substantial that it can justify such

[129] Datatisynet, 'Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion' (24/05/2019) <https://www.datatilsynet.dk/afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion> (Accessed 13th November)

[130] Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven), LOV nr 502 af 23/05/2018, § 7(4)

[131] Hutchins, Brett, and Mark Andrejevic. "Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring." *International Journal of Communication* 15 (2021): 363-82., p. 370

[132] Ibid (Hutchinson, Brett, and Mark Andrejevic), p. 370

intrusion on all the other spectators, especially children? The processing of special categories of data should only be when it is necessary to achieve the purpose of the controller, and the controller should exhaust the other methods for achieving that purpose priorly. The football club could potentially use another method for identifying the banned spectators, such as selling tickets with names on or demanding IDs at the entrance to the stadium.

One can, as in the previous scenario, utilize the right to object. It is unknown if the football club would comply with an objection, however the objection would force the club to assess the balance of interest and present a compelling legitimate ground for such processing which override the rights and freedoms of the data subject. As discussed, the particular reason of individuals may differ substantially: some might be excessive or unfounded, others may be reasoned and justifiable. Those who object just because they can, will generally not have a justifiable ground. If a spectator with a social impairment or physical disability submits an objection, then a careful assessment of the balancing test will have to be conducted. The interference of privacy may be so invasive to some individuals that they refrain from participating as spectators.

If the objection is justified and the football club subsequently would have to stop the processing of one single individual, it can be difficult to organise so that the cameras will not capture footage of that individual in the future. In addition, it can signal to other spectators that they may submit an objection in order to avoid the facial recognition cameras. If enough spectators utilize their right to object, then the purpose of deploying the cameras would dematerialize. On the other hand, the individuals who are banned from the stadium would most likely not have a substantial ground for rejecting the processing as it might be unfounded. Either way, if the football club would have to approve an objection, the purpose for processing such data might diminish.

5.2 Swedish Skellefteå High School – facial recognition based on consent

The high school in Skellefteå in Sweden, which was previously mentioned, ran a pilot program which documented students' attendance through surveillance cameras with facial

recognition.[133] Students could decline to participate in the project, and an explicit consent was required from the students who wished to participate. There were 22 students participating in the project, and their parents had consented priorly to the processing of personal data.

Deploying facial recognition cameras to document students' attendance is not a necessary measure in order to check the attendance. The high school argued that although such processing was not necessary, the automating of the class register would save the school from 17280 hours of work each year.[134] The use of facial recognition cameras constituted the processing of biometric data which are extra worthy of protection and an explicit exception under Article 9 (2) is required in order to conduct such processing. [135] The high school relied on the explicit consent from the student's parents in order to process the biometric data under Article 9 (2)(a) GDPR. The Swedish data protection authority assessed that whether the consent could constitute a 'freely given' consent could not only be based on the students' freedom of choice, but also the relationship that exists between the students and the school as a controller.[136] It empathised that within the school area, the students are dependent on the school in terms of education, grades and scholarships, hence a student's consent could not be properly 'freely given'. In contrast it was established that consent could be used as a legal bases for certain other types of processing of personal data within the school, such as when photographing of the students and documenting school activity.

This case provides a strict approach to the 'explicit consent'. Although it is in line with the regulation, especially while considering the sensitivity of the data being processed, it raises the question of when a consent could be valid. The 'explicit' consent will rarely be freely given in a relationship as the present, and as such it will be invalid. Nevertheless, how can a student take part in the project if it really wishes to? In some situations, it might be preferable for a person to be subject to processing. The students in this case would, for instance, save time and trouble on the class register by having the facial recognition cameras automatically registering their attendance. In addition, it might be in the students' own interest to take part in a program for

[133] Datainspektionen, 'Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever'(20/08/2019) <https://www.imy.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf> (accessed 10th November 2021)

[134] Ibid, *Datainspektionen*, p.3

[135] Ibid, Datainspektionen,

[136] Ibid, *Datainspektionen*, p.5

academic purposes. It seems unlikely that the students would be able to make a valid consent, however it should arguably be a method for the students to become subject to such processing if they really wish to.

Furthermore, the processing of biometric data would generally have to find an exception under Article 9 (2) and a lawful ground under Article 6. The high school argued that the processing could be based on the lawful ground of public interest, Article 6 (1)(e), however this was rejected by the Swedish data protection authority. The high school could potentially have relied on the lawful ground of legitimate interests if it had been a private entity. The Danish case above could, as in the present case, use less intrusive methods for achieving its purpose, however it was still allowed to conduct the processing by the Danish data protection authority. Should the high school therefore also be permitted to continue the processing?

5.3 VoetbalTV – legitimate interest

A Dutch company, VoetbalTV, was fined by the Dutch data protection authority for failure to establish a lawful ground for processing.[137] The company conducted video recordings and live streamed football matches and trainings on behalf of armature football clubs. The football clubs had to sing up for the service, and their players and coaches could subsequently analyse, watch and share the matches with each other through a channel which one would have to subscribe to. As this case concerned amateur football, the purpose of processing though video devices was not sufficient to meet the journalistic exception, such as where premier league football matches are live streamed on TV, hence the processing was based on the ground of legitimate interest. The Dutch Data Protection Authority, on the other hand, found that the company's processing was based on a commercial interest which was insufficient and could not constitute a legitimate interest.

The decision was later taken to court, and the Dutch data protection authority's decision was declared invalid. The court pointed out that it is up to the controller to assert what legitimate

[137] De Rechtspraak, 'VoetbalTV hoeft boete Autoriteit Persoonsgegevens niet te betalen' (23th November 2020) https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Midden-Nederland/Nieuws/Paginas/VoetbalTV-hoeft-boete-Autoriteit-Persoonsgegevens-niet-te-betalen.aspx (accessed 11th November 2021)

interest it has (which is a non-exhaustive list), and the decision that follows must rather be based on the conclusion of the balancing test and necessity for processing.[138] The court did not discuss the legitimacy of the company's processing of personal data, however, and rather focused on the procedure data protection authorities had to follow when determining whether a lawful ground for processing exists.[139] As discussed earlier, legitimate interest can be based on commercial interest, especially where there is additional interests in conducting the processing. Players, coaches, families, and friends constitute third parties which would benefit from and enjoy the video service presented by the company, thereby presenting an additional interest. The processing of personal data though video device systems are also necessary in order to achieve the purpose of conveying the matches and trainings. There are no other alternatives to achieving that purpose. When balancing the interest of the company and the third parties against the objective reasonable data subject, there is an assumption that the company's interest may be legitimate.

Nevertheless, the data subjects can object to the processing of their personal data if the processing is found to be lawful under Article 6 (1)(f). As discussed earlier, what is a 'particular situation' or the 'compelling legitimate ground'? VoetbalTV deploy video cameras to record practices and matches in order to better the performance of the players and to live stream and upload the matches online. There might be one out of all the players which object to being recorded, while the rest of the players are in favour of the video cameras. During times like covid-19 where family, friends and fans have not been able to watch matches and competitions, live streaming and video recordings could be of great value and in the interest of both the audience and the players. If the one player's objection would override the club and the other players' interest, then it would result in that video footage would have to be deleted and the controller would have to cease to record.

The 'particular situation' of the data subject can vary, and each objection must be decided on a case-by-case basis. The player's 'particular situation' will thereby be assessed in order to balance the rights of all parties in a fair and reasonable manner in accordance with the principle of proportionality. Where the player has a handicap, is in a wheelchair or is young, then that

[138] Central Netherlands Courts, *VoetbalTV BV v. Dutch Data Protection Authority*, Case number: *UTR 20/2315* (23/11/2020)

[139] Ibid, *VoetbalTV*

person's particular situation might weigh heavily, especially where the person would stop playing if the video recording continues. On the other hand, where the player has no particular reason, or the objection seems manifestly unfounded or excessive, then the controller could refuse to comply with the objection and continue the processing of the video footage. Provided that a player's objection is rejected by the controller, the processing of personal data through the video devices could potentially result in players quitting.

5.4 Summary

Although the cases above are different and have adopted different approaches to the lawful grounds for processing, it can indicate that processing of personal data though video device systems are regulated differently throughout the European Union. Sweden, on one hand, struck down the deployment of facial recognition cameras instantly in order to set a precedence. Denmark, on the other hand, has allowed for facial recognition cameras for the entrance to a football stadium run by private actors, regardless of the fact that there are less intrusive methods for achieving the actors' purpose. In the Netherlands, the Dutch data protection authority misinterpreted the regulation to be applied under the GDPR, and was subsequently corrected by the courts of Netherlands. Although all cases are different, one can presume that the processing of personal data through video device systems conducted by private entities are subject to vague regulation which leads to differing interpretations.

As was recognised by the Swedish data protection authority when it concluded its judgement; technology is devolving quickly, and there is a great need to create clarity about what applies to all actors that wish to deploy cameras with facial recognition. The same should be applied to all private actors wishing to process personal data through video devices across Europe.

5.4.1 Recommendations

5.4.1.1 Harmonizing the rules

GDPR was intended to harmonize the laws and regulations relating to personal data across the EU and all Member States. It does, however, seem like the GDPR is interpreted and applied in different ways. This indicated that the rules relating to the processing of personal data through video devices by private actors are not sufficiently clear. Considering how quickly the

technology is developing, where smart cameras are likely to become commonly deployed by private actors, it is important that all the rules relating to such processing are subject to proper and comprehensive guidelines. It is therefore proposed that such guidelines are issued and that data protection authorities are properly prepared and organised in order to guide private companies, in addition to holding them accountable.

6 Conclusion

General legislation should be unchallenging to interpret and understand in order for people to adhere to it. Most people wish to be law-abiding citizens and do their best to follow the rules laid out by the state and community they belong to. In addition, people will generally strive to avoid getting fines and penalties. All legislation is up for some sort of interpretation. For instance, if one kills another person, there are multiple factors that would contribute in the assessment of conviction. Factors such as if it was an act of self-defence, manslaughter, or an accident will help in determining the seriousness of the crime. Nevertheless, everyone understand that a crime has happened, and that murder is illegal. It is important to have legislation which clearly sets out unambiguous rules and regulation for people to follow. If something is deemed to be illegal, people tend to avoid it.

The processing of personal data through video devices is intrusive on the data subject in nature. The data gathered can potentially identify and map out individuals' habits and personal characteristics that the data subject wish to keep private, which may result in an interference with human rights. It is therefore paramount to have unambiguous regulation and clear guidelines concerning the use of camera devices and the processing of data that follow. A balancing test will rarely meet the conditions for a straightforward and unambiguous regulation. The balancing tests are obscure in the sense that every case must be decided on a case-by-case basis, and there is no proper answer to the outcome. The possibility of an unpredictable decision is generally not in the best interests of neither the controller nor the data subject. In addition, it can be complicated for the interested parties to adhere and follow the regulation. In some instances, the parties might simply make a decision and await a possible interference by the national data protection authority, in order to truly know if the processing is justified or not. The lack of judicial precedence and the vague notion of 'balancing of interest' can make it difficult for private controllers and data subjects to understand their rights and interests. As

evidenced from the cases discussed, the rules relating to the processing of data though video devices are interpreted and applied in different ways. The number of private companies processing personal data by deploying video devices are still limited, however as a result of the developments in technology it is likely to increase. It is therefore relevant to establish clear-cut rules which is easy to apprehend and adopt.

Nevertheless, considering that every case is unique and that all interests at stake must be assessed, a balancing test is undoubtedly an appropriate approach in order to reach a justifiable decision. There is no simple answer to what extent the balancing tests will ensure an appropriate and proportionate balance between the rights and interests of the data subject and the controller concerning the processing of personal data through video devices. The balancing test following the 'legitimate interest' is fairly developed, and it should not be complicated to establish a legitimate interest considering that the legitimate interest list is non-exhaustive. The processing of personal data through video devices is, however, quite intrusive on the data subject, thus it might be necessary to develop additional safeguards for the data subject. The increase in technological developments will likely expand the use of video devices, and such expansion should be recognised in the balancing test. One issue which arise for both the balancing tests is that the assessments are to be conducted by the controller, which can affect the objectivity of the assessment. Considering that all people are different, there is a possibility that that balancing tests can never be properly objective, and can in principle be to the detriment of the data subject. The national data protection authorities could serve as an objective third party, and can potentially become more involved where the balancing tests are conducted.

The right to object is, similarly to the lawful ground of 'legitimate interests', subject to a balancing test. The right to object complements the balancing test of rights and interests in the sense that where processing is allowed, the data subject still has an additional possibility to avoid processing. Although the application of the balancing test is fairly justified by the fact that each individual will submit an objection based on its subjective 'particular situation', the balancing test has multiple weaknesses resulting from the vague definitions and guidelines on the right to object. Firstly, the legislation and guidance on the right to object does not properly address what constitute a 'compelling legitimate ground' or a 'particular situation'. In addition, the threshold for a 'particular situation' is not established, and neither is the threshold for a 'compelling legitimate ground'. Can a data subject simply object because of an obscure reason, or must the controller's rejection be based on a crucial interest in order to override the data

subject's rights and freedoms? Lastly, it must also be clarified whether third party interests are included, and to what extent they are influencing the balancing test. The balancing test is of great value considering that every case is unique, however it requires clear and comprehensive guidance on where objections can be justified or not. The balancing test cannot be applied in an appropriate and proportionate manner without proper definitions and guidance of the rights and interests to be balanced.

The balancing tests are an appropriate approach in order to balance all the interests and rights at stake. Nevertheless, without proper guidelines and definitions in place, it can be difficult to achieve a balancing test which ensures an appropriate and proportionate balance between the data subject's rights and controller's interests.

Table of reference

Statutes:

i. Charter of Fundamental Rights of the European Union (2000/C 364/01)

ii. 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.

iii. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) (1953)

iv. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive)

v. 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)

Judgements:

i. *Big Brother Watch & Others v. The United Kingdom* (ECtHR, 13 September 2018) §387.

ii. Central Netherlands Courts, *VoetbalTV BV v. Dutch Data Protection Authority*, Case number: *UTR 20/2315* (23/11/2020)

iii. Judgement of the CJEU, 6th November 2013, *Bodil Lindqvist case*, Case C-101/01,

iv. Judgment of the CJEU, 11th December 2014, *František Ryneš v Úřad pro ochranu osobních údajů*, C-212/13, ECLI:EU:C:2014:2428

v. Judgment of the CJEU, 11th of December 2019, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064

vi. Judgment of the CJEU, 13 May 2014, *Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, no. C-131/12, ECLI:EU:C:2014:317 (‘*Google Spain*’)
vii. *Peck v. United Kingdom*, App No 44647/98, ECHR 2003-I, [2003] ECHR 44, (2003) 36 EHRR 41, (2003) 36 EHRR 719.
viii. Judgment of the ECHR, 4th May 2017, *Rīgas satiksme*, Case C-13/16

Publications from authorities:

i. Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217 (9 April 2014)
ii. Article 29 Working Party, Overview of results of public consultation on Opinion on legitimate interests of the data controller (Opinion 06/2014)
iii. Datainspektionen, ‘Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever’(20/08/2019) <https://www.imy.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf> (accessed 10th November 2021)
iv. Datatisynet, ‘Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion’ (24/05/2019) <https://www.datatilsynet.dk/afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion> (Accessed 13th November)
v. EDPB 2019B: European Data Protection Board,‘Guidelines 3/2019 on processing of personal data through video devices‘ (10 July 2019).
vi. European Data Protection Board, ‘Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)’ (7th July 2020), p.9
vii. Information Commissioner’s Office, “Guide to the General Data Protection Regulation (GDPR)” (2018)
viii. Information Commissioner’s Office, “What is valid consent?” < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what5> (accessed 12th November 2021)

Books:

i. Hutchins, Brett, and Mark Andrejevic. "Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring." *International Journal of Communication* 15 (2021): 363-82., p. 370

ii. Kuner, Christopher, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler, eds. *The EU General Data Protection Regulation (GDPR): A Commentary*. New York: Oxford University Press, 2020. Oxford Scholarship Online, 2021. doi: 10.1093/oso/9780198826491.001.0001.