Administrative enforcement of data protection law in Norway in the years between 2001 and 2019

An assessment of some of the most criticized and questionable legal positions acquired by the Data Protection Authority and the Privacy Appeals Board in the field of data protection law in the years between 2001 and 2019

Candidate number: 7013

Submission deadline: 01.12.2019

Number of words: 17478
# Table of contents

1 INTRODUCTION .................................................................................................................. 4
   1.1 Presentation of the topic .................................................................................................. 4
   1.2 Research question ......................................................................................................... 5
   1.3 Methodology .................................................................................................................. 5
   1.4 Scope .................................................................................................................................. 6
   1.5 Overview .......................................................................................................................... 7

2 AN INTRODUCTION TO THE NORWEGIAN ADMINISTRATIVE ENFORCEMENT SYSTEM RELATING TO DATA PROTECTION LAW ........... 8
   2.1 Proceedings in the administrative system ....................................................................... 9
   2.2 Proceedings in the court system ................................................................................... 10

3 LEGAL POSITIONS ACQUIRED BY THE DATA PROTECTION AUTHORITY 11
   3.1 An introduction to the Data Protection Authority .......................................................... 11
   3.2 Legal positions concerning case dismissals ................................................................... 13
      3.2.1 Explaining the problem ......................................................................................... 13
      3.2.2 Down-prioritizing a case without making a formal decision to dismiss ................. 15
      3.2.3 May the Authority dismiss a case based on a lack of resources? ...................... 15
   3.3 Legal positions concerning the Police Databases Act .................................................. 18
      3.3.1 Explaining the problem ......................................................................................... 18
      3.3.2 The Authority’s competence relating to the Police Databases Act ....................... 19
      3.3.3 Procedural elements in the case PVN 2018/17 ...................................................... 19
      3.3.4 Material elements of the case PVN 2018/17 - should the Authority have reacted to the Police’s processing? ................................................................. 21

4 LEGAL POSITIONS ACQUIRED BY THE PRIVACY APPEALS BOARD .......... 23
   4.1 An introduction to the Privacy Appeals Board ............................................................... 23
   4.2 Disagreements between the Authority and the Board .................................................. 25
      4.2.1 Explaining the problem ......................................................................................... 25
      4.2.2 Legal positions concerning the processing of data relating to criminal convictions ..................................................................................................................... 26
      4.2.3 Legal positions concerning the scope of consent .................................................. 33
4.2.4 Camera surveillance ................................................................. 41

4.3 Legal positions concerning the Police Databases Act ........................................ 48

4.3.1 Section 60(1) and (2) of the Police Databases Act – processing in connection with or not in connection with a criminal case? .................................................. 49

4.3.2 Section 60(3) of the Police Databases Act – may the claimant appeal a decision which establishes lawful processing? .................................................. 53

5 CONCLUSION ......................................................................................... 56

6 TABLE OF REFERENCE ........................................................................ 57
1 Introduction

1.1 Presentation of the topic

Enforcement is the backbone of the rule of law. It is the connecting factor from a right de jure to a right de facto. The EU Commission has in the GDPR recognized the significance of enforcement, in which the GDPR must be “backed by strong enforcement” in order to create trust which enables the purposes of the GDPR to be achieved.\(^1\) One of the two main purposes of data protection law is to protect natural persons with regards to the processing of personal data\(^2\). This protection is dependent on how the enforcing agencies establish data protection law de lege lata, thereunder the scope and character of the data subject’s rights on a case-by-case basis.

The administrative enforcement system of data protection law is especially interesting in a Norwegian context. It consists of the Data Protection Authority (“the Authority”) and the Privacy Appeals Board (“the Board”). These two agencies have a significant impact on data protection law de lege lata. This is because they handle the clear majority of data protection cases in Norway\(^3\), in addition to handling a vast variety of legal issues\(^4\).

Data protection law de lege lata consists of legal positions acquired by the Authority and the Board. Some of these legal positions have remained through several years, while some are relatively new. Many have been challenged by one data protection enforcement agency directed to another, and some have been challenged by external public institutions having an interest in the enforcement of data protection law. Some legal positions are also funded on a questionable line of arguments and a noteworthy legal method.

One might disagree with the following assessments. The involved parties have acquired different positions based on more or less the same sources of law, which illustrates the complicated nature

---

1. Recital 7 GDPR
2. Cf. Article 1(1) GDPR and the EEA cf. the EEA Agreement appendix XI no. 5e. The other is to ensure free movement of data within the EU.
3. 3070 decisions from the Authority 2013-2018 (there are no metadata on the amount of decisions made before this and in 2019), 272 appeals to the Board between 2001-2019 and 148 judgements in the court system between 2001-2019 relating to the Personal Data Act 2018 and 2000, in which most of the court’s decisions are primarily connected to other fields of law
4. The court’s cases have mainly concerned control measures and compensation
of the relevant fields of law. The aim of the following discussion is however not to conclude whether or not the Authority and the Board have been right or wrong, but to problematize their legal positions in light of other legal positions and in light of the surrounding sources of law.

1.2 Research question
This thesis will explore some of the legal positions acquired by the Authority and the Board between the years 2001\(^5\) and 2019 which have either been subject to criticism, or have been based on questionable arguments and legal method. These legal positions will be assessed in light of the agencies’ own reasoning, criticism from one agency to the other, criticism from external public agencies and available sources of law.

All of the above lead towards the question of whether or not the agencies have misinterpreted fundamental legal concepts, or misunderstood factual circumstances vital for the interpretation of the relevant legal framework.

1.3 Methodology
The research for this thesis has mainly been based on publicly available case law, namely the Board’s appeals cases\(^6\). Both the Authority’s and the Board’s legal positions are to a certain degree explained in these documents.

Some legal positions have not been sufficiently elucidated through this case law alone, which has required a number of access requests directed to the Authority, the National Criminal Investigation Service, the National Police Directorate and the Justice Department. Telephonic and personal meetings with representatives from the Authority, the current Board\(^7\), the Police Directorate and the Justice Department have also been necessary.

---

\(^5\) The Board was established in 2001
\(^6\) The Privacy Appeals Board “Decisions” [https://www.personvernemnda.no/avgjorelser](https://www.personvernemnda.no/avgjorelser) Retrieved 31.10.2019
\(^7\) The Board composition elected for the period 2017 to 2021.
As for the legal frameworks used in this thesis, both the prior data protection framework\(^8\) and the currently applicable data protection legal framework\(^9\) have been relevant. The Public Administration Act and the Police Databases Act have also been important sources of law relating to some of the issues presented.

A methodological challenge has been that the Authority’s and the Board’s legal positions have been difficult to compare at times as they have not always been based on the same provisions.

### 1.4 Scope

As already mentioned, the enforcement of data protection law is best illustrated through looking at the Authority’s and the Board’s case law. An assessment of the court’s case law is therefore excluded from this thesis.

The analysis will be based on primarily three legal frameworks: The Personal Data Act of 2000 and 2018, the Police Databases Act and the Public Administration Act. The Personal Data Acts represent the general data protection framework. The Police Databases Act represents a rather specialized field of data protection law. The latter represents a particular challenge for both the Authority’s and the Board’s fundamental understanding of data protection law and their ability to familiarize themselves with complicated factual circumstances. The Public Administration Act is an underlying fundamental field of law that is necessary for the interpretation and general enforcement of both legal frameworks.

As for the relevant general data protection regimes in this thesis, I have chosen to address the interpretation of both the prior data protection framework \textit{and} the currently applicable framework. This is due to the fact that the two legal frameworks are similar to a high degree, which means that the considerations relating to the prior data protection framework are generally of interest to the interpretation of the currently applicable data protection framework. The GDPR is indeed more detailed than the Personal Data Act of 2000\(^10\), but the character of the different rights and duties

\(\)\(^8\) The Personal Data Act 2000 and the Data Protection Directive
\(\)\(^9\) The GDPR cf. the Personal Data Act 2018 section 1
\(\)\(^10\) Rønnevik et al. (2019) page 41
remain largely the same. There is also an inherent value to analyzing the way in which the Authority and the Board interpret and enforce the at all times applicable legal framework.

1.5 Overview

Section 1 introduces the subject and structure of this thesis.

Section 2 elaborates on the procedure of a data protection case in Norway. This includes the court system for the purpose of providing a complete picture of the enforcement mechanism. This elaboration is necessary to clarify the relationships between the involved agencies and their roles in a general sense.

Sections 3 and 4 provides the actual analysis of the Authority’s and the Board’s practice. Each section involves a general introduction of the relevant agency’s purpose and organization, leading to the assessment of the relevant legal positions.

Section 5 provides concluding remarks on the basis of the assessments provided in respectively sections 3.2 and 3.3, as well as 4.2 and 4.3.
An introduction to the Norwegian administrative enforcement system relating to data protection law

The subject of this thesis, namely the enforcement of data protection law in the Norwegian enforcement system, requires an explanation of data protection proceedings in the administrative system. The following figure is a visual representation of this procedure.

The prerequisite of a data protection procedure is typically that the data subject suspects that someone is processing his or her data in violation of the applicable data protection legal framework\textsuperscript{11}. He or she can bring this matter to either the courts or to the Authority. The data subject is not required to empty the administrative appeals system before bringing the case to the courts.\textsuperscript{12} However, the Authority is often the preferable starting point as it is free of cost\textsuperscript{13}, and because court proceedings may be more time-consuming. Further, the Authority and the Board has a general duty to provide guidance\textsuperscript{14} and to assess the case on an individual basis\textsuperscript{15}.

\begin{itemize}
  \item The procedure may also be initiated on the basis of the Authority’s independent activities, see section 2.1
  \item This may be interpreted from the term “without prejudice to any other administrative or non-judicial remedy” cf. Articles 77, 78 and 79 GDPR
  \item This is required by law cf. Article 57(3) GDPR stating that «The performance of the tasks of each supervisory authority shall be free of charge for the data subject»
  \item Cf. section 11 of the Public Administration Act. As for the Board, this is also specifically mentioned in section 2 in the Instruction for the Privacy Appeals Board
  \item Cf. the principle of clarification enshrined in the Public Administration Act section 17(1) first sentence
\end{itemize}
2.1 Proceedings in the administrative system

Proceedings in the administrative system may be initiated in different ways, in which the Authority is the starting point. Usually, a data subject directs a claim to the Authority. The Authority will then establish a case on the basis of this complaint. Many of the cases established in the Authority are also established on the basis of independent supervisions conducted by the Authority.

After a case is established in the Authority, the Authority must make a decision, which is legally binding upon the involved parties. The Authority may (i) dismiss the case, (ii) refuse the claim or (iii) approve the claim. Either of the parties may appeal the Authority’s decisions. The Authority will first try their own decision, and pass the case to the Board if they uphold their original decision.

The Board shall assess the case on an individual basis, and may, alike the Authority’s mandate, either (i) dismiss, (ii) refuse or (iii) approve the claim. The Board further has a mandate to pass the decision back to the Authority on their own discretion, typically when they claim that the

---

1. Cf. Articles 57(1) f) and 77(1) GDPR
2. Cf. Article 57(1) a) GDPR
3. Cf. section 2(1) a) of the Public Administration Act
4. Cf. section 22 of the Personal Data Act 2018 and Article 78 GDPR
5. Cf. the principle of clarification enshrined in the Public Administration Act section 17(1) first sentence
6. Ibid. section 35(2) cf. (1), stating that “the administrative decision may also be reversed by the appellate instance” on its own initiative if certain conditions are fulfilled.
Authority has not assessed the case well enough\textsuperscript{22}. The case may in principle be sent back and forth between the Authority and the Board multiple times\textsuperscript{23}, but the consideration for effective case management\textsuperscript{24} limits the time frame of a case.

Administrative decisions made by the administrative agencies are legally binding on the parties when the deadline to appeal has past\textsuperscript{25} and the deadline for the first or appellate agency to reverse the decision has past\textsuperscript{26}.

\textbf{2.2 Proceedings in the court system}

A data protection case may be brought to the courts independent of any procedures in the administrative enforcement system when the data subject “considers that his or her rights under (the GDPR) have been infringed”\textsuperscript{27}. The court proceedings are not affected by whether or not the relevant claim has been proceeded in the administrative system beforehand.

\begin{itemize}
  \item \textsuperscript{22} This was the case in PVN 2009/20, PVN 2014/15 and PVN 2016/03
  \item \textsuperscript{23} In for example PVN 2016/03, the Authority asked the Board not to send the case back, because it had already been in the Authority twice.
  \item \textsuperscript{24} Eckhoff (2019) page 203, Graver (2015) page 275
  \item \textsuperscript{25} Cf. section 29 of the Public Administration Act
  \item \textsuperscript{26} Ibid. section 35(3)
  \item \textsuperscript{27} Cf. Article 79(1) GDPR
\end{itemize}
When the claim is brought to the courts, the relevant district court will assess whether or not the general requirements for admitting a case before the courts are fulfilled\textsuperscript{28}. After the district court has made a judgment, the case may be appealed to the circuit court, and further to the Supreme Court if accepted by the Supreme Court’s Appeals Committee\textsuperscript{29}.

The case is legally binding on the parties when it cannot be “challenged by exercising an ordinary legal remedy”\textsuperscript{30}, typically by appealing.

If a legally binding judgement from the court system exists, one might wonder if this case may be brought to the Authority. In the case PVN 2018/01, the Authority decided not to make an individual assessment because “to make a decision pursuant to the Personal Data Act section 46 seems like an inexpedient use of the Authority’s resources, when this case is already handled in the court system.” The Authority decided that the courts made an “individual and thorough assessment”, and supported it thereof. As such, there is nothing in the way of bringing the case to the Authority after having it decided by the courts. Yet, the case will most likely end with the same result.

3 Legal positions acquired by the Data Protection Authority

3.1 An introduction to the Data Protection Authority

The Authority makes a vast amount of decisions every year\textsuperscript{31}. All of these decisions have a significant impact on the rights and duties of the relevant private individuals, public agencies and corporations. Their legal positions should therefore be subject to scrutiny in order to lay the foundation for optimal data protection.

\textsuperscript{28} The Civil Procedure Act defines this requirements, especially chapters 1 and 2

\textsuperscript{29} Cf. the Civil Procedure Act section 30-2 and The Criminal Procedure Act section 323. The case typically has to be of principle meaning.

\textsuperscript{30} Cf. section 19-14(1) of the Civil Procedure Act

The Authority is established as Norway’s supervisory authority. Its function is to “be responsible for the application” of the GDPR, and its purpose is to “protect the fundamental rights and freedoms” of data subjects and to “facilitate the free flow of personal data” within the EU.

The Authority is an independent administrative agency, subordinate to the “King” and the Ministry of Local Government and Modernisation. The fact that they are an independent administrative agency means that they cannot be instructed about the proceedings in cases or the general day to day operations. Additionally, neither the government nor the ministry may overturn the decisions made by the Authority.

The Authority has a mandate to handle all cases relating to the Personal Data Act, cases relating to the Police’s and the prosecuting authority’s processing activities, health registries and certain cases relating to the Schengen Information System (SIS). The majority of the Authority’s decisions relates to violations of the controller’s and processor’s duties enshrined in the GDPR, more precisely a lacking internal control of processing activities.

---

32 Article 51(1) GDPR states that Member States, including Norway cf. section 1 of the Personal Data Act 2018, must provide for one or more “independent public authorities” to be responsible for “monitoring the application of this Regulation”.

Section 20(1) of the Personal Data Act 2018 states that the Authority is the supervisory authority cf. Article 51 of the GDPR.

33 Article 51(1) GDPR

34 Ibid.

35 Cf. section 20(1) of the Personal Data Act 2018 stating that “The Data Protection Authority is an independent administrative body subordinate to the King and the Ministry.”

36 In reality the government

37 Cf. section 20(2) of the Personal Data Act 2018

38 Ibid. section 20(1) stating that “The King and the Ministry may not issue instructions regarding or reverse the Data Protection Authority’s exercise of authority in individual cases pursuant to statute.”

39 Ibid. section 22 (1)

40 Ibid. section 20(3) a)

41 Cf. section 58 of the Police Databases Act section 58 and section 42-1 of the Police Databases Regulation

42 Cf. section 26 of the Personal Health Data Filing System Act

43 The authority competence is described in section 21(1) and (2) of the SIS Act

44 This is mentioned in the Authority’s yearly report from 2018 page 14. Such internal controls typically relate to the duty of implementing “appropriate technical and organizational measures” cf. Article 24(1) GDPR and to keep records of processing activities cf. Article 30(1) and (2) GDPR.
3.2 Legal positions concerning case dismissals

3.2.1 Explaining the problem

Case dismissals has been a recurrent subject of critique from the Board\textsuperscript{45}. This critique relates more specifically to (i) the fact that the Authority on several occasions has “down-prioritized” cases without making a formal decision to dismiss, and (ii) dismissing a case based on a lack of resources.

The Board’s critique is manifested in both yearly reports and individual cases.

In the yearly report from 2014, the Board wrote the following: “a recurrent issue is the Authority’s lack of individual assessment in individual cases in the form of down-prioritization without an administrative decision or decision to dismiss.” The same was repeated in the yearly reports from 2016 and 2017.

The criticism is also expressed in the following cases, amongst others\textsuperscript{46}:

In the case PVN 2013/26, the claimant requested the Authority to assess the lawfulness of Mittanbud.no’s processing of his personal data. The Authority claimed they did not have a duty to perform a control and subsequent individual assessment in every case in which they received a complaint about possibly unlawful processing of personal data. They decided to down-prioritize the case, without making an individual assessment in the case or a decision to dismiss.

The Board claimed that the Authority should have made a formal decision to dismiss, because a decision not to make an individual assessment in the case is decisive for a person’s rights and duties. It was therefore subject to appeal\textsuperscript{47}.

\textsuperscript{45} The critique is presented in the Board’s yearly reports and specific cases. These sources are further elaborated below.

\textsuperscript{46} The criticism is also mentioned in connection with the cases PVN 2017/05, 2017/15, 2017/09, 2016/13, 2016/03, 2015/17, 2015/03, 2014/07, 2014/06, 2014/05 and 2013/26

\textsuperscript{47} Cf. section 2(1) a) of the Public Administration Act, cf. section 22(1) of the Personal Data Act 2018
In the case PVN 2016/03, the dispute was a neighbor’s alleged unlawful camera surveillance of the claimant’s private property. The Authority first decided not to make an individual assessment in the case due to lack of resources. The claimant appealed, and the Authority once again decided not to make an individual assessment. The claimant requested the Authority to make a decision to dismiss the case, which was subsequently denied. The Authority further claimed that the decision could not be appealed, as down-prioritizations were not “administrative decisions” cf. section 2(1) a) of the Public Administration Act.

The Board once again\textsuperscript{48} stated that the Authority should have made a formal decision to dismiss, and that the claimant has a right to appeal the case. The Authority later admitted that they should have made a decision to dismiss. The Board also claimed that the Authority cannot choose \textit{not} to make an individual assessment in a case and thus down-prioritize it, based on a lack of resources.

In the case PVN 2018/01, Keolis, a company drifting the tram in Bergen, used three security video recordings for the dismissal of a tram driver. The Authority chose not to make an individual assessment in the case, nor make an administrative decision to dismiss, as the case had been handled by the district court. It was allegedly a waste of resources to make an individual assessment in the case.

The Board stated again\textsuperscript{49} that the Authority cannot “choose not to address the material questions in the case”, and that prioritization of resources only gives a certain power to choose how thorough a case should be assessed.

\textsuperscript{48} The first time was in the case PVN 2013/26

\textsuperscript{49} The first time was in the case PVN 2013/03
3.2.2 Down-prioritizing a case without making a formal decision to dismiss

As for the first point of criticism, “down-prioritizing” a case is in effect the same as dismissing a case\(^{50}\). Not making a formal decision to dismiss when in fact dismissing a case threatens the data subject’s right to an appeal\(^{51}\).

The reason for this is that the absence of a formal decision to dismiss may deprive the case of the status of an “administrative decision”\(^{52}\), which is the requirement for an appeal to the Board\(^{53}\). As such, if the Authority chooses to down-prioritize a case, they must subsequently make a formal decision to dismiss.

3.2.3 May the Authority dismiss a case based on a lack of resources?

As for the second point of criticism, dismissing a case based solely on a lack of resources may violate the Authority’s duties pursuant to the Public Administration Act. This is a repeated matter in the Authority’s practice. The fact that this practice has remained over several years, in spite of a routine in which the Authority adopts the Board’s legal positions unless they disagree\(^{54}\), suggests that the Authority and the Board are on opposite positions as a matter of principle. The following is an attempt to clarify which position is in line with the surrounding legal framework.

The Authority has used their discretion to dedicate resources in support of their view that they may dismiss cases based on a lack of resources\(^{55}\). The Board is of the opinion that this discretion does not allow the Authority to simply choose not to make an individual assessment of the material questions in the case\(^{56}\), and must rather dedicate less resources in the individual assessment.

\(^{50}\) Down-prioritizing a case and dismissing a case both result in the claimant not having his claim assessed on an individual basis. Down-prioritizations shall therefore be considered “administrative decisions” on the same level as formal dismissals cf. sections 2(1) a) and 2(3) of the Public Administration Act. This means that down-prioritizations are also subject to appeal cf. section 22(3) of the Personal Data Act 2018.

\(^{51}\) Cf. section 22(2) of the Data Protection Act 2018 and Article 78(1) GDPR

\(^{52}\) Cf. section 2(1) a) of the Public Administration Act

\(^{53}\) Cf. section 22(3) of the Personal Data Act 2018

\(^{54}\) This routine was mentioned during a meeting with a representative from the Authority in October

\(^{55}\) This is recognized by the Board in for example PVN 2018/01

\(^{56}\) Stated in PVN 2018/01 and PVN 2016/03
The Authority’s discretion relating to resource management is most likely derived from the clarification duty in section 17(1) of the Public Administration Act. The clarification duty entails that an administrative agency must “ensure that the case is clarified as thoroughly as possible before any administrative decision is made”. Article 57(1) f) GDPR states similar to this that the Authority must “investigate, to the extent appropriate, the subject matter of the complaint”.

The clarification duty must be interpreted in accordance with the relevant agency’s resources cf. the terms “as possible”\(^\text{57}\) and “to the extent appropriate”\(^\text{58}\). Eriksen and Fredriksen support that resources are determinative for the interpretation of the clarification duty.\(^\text{59}\)

Yet, these terms do not necessarily solve the question of whether or not a complete lack of resources allows to refrain from an individual assessment. They seem to address the question of the extent of resources which should be put into an individual assessment, but not necessarily whether or not dedicating none at all is an option.

However, the mere existence of a clarification duty relating to an administrative decision entails that an administrative decision must always be based upon some form of individual assessment.

Bernt claims that the clarification duty gives the relevant agency “an independent responsibility to assess the quality and the accountability of the information it receives, especially those provided by the parties to the case”\(^\text{60}\). This leads in the direction that the Authority must always make an individual assessment at least to the extent that the material presented by the parties is quality checked.

Another source of interpretation is the fundamental two-body structure in the administrative system. This structure is reflected in section 22(3) of the Personal Data Act 2018: “The Privacy Appeals Board shall decide appeals against the decisions of the Data Protection Authority”. The

\(^{57}\) Section 17(1) of the Public Administration Act  
^{58}\) Article 57(1) f) GDPR  
^{59}\) Eriksen and Fredriksen (2019) page 109  
^{60}\) Bernt (1967) comment no. 477
Authority must make “decisions” within the meaning of “administrative decisions” cf. section 2(1) a) of the Public Administration Act, in order to maintain the two-body structure.

On the one hand, dismissals are also “administrative decisions” as stated above. This could suggest that the two-body structure is maintained also when the Authority dismisses cases without making an individual assessment based on a lack of resources.

On the other hand, an “appeal” within its natural meaning presupposes that the first instance has made an actual assessment of the case which one may disagree with and thus appeal. The Board is established as an appeals institution\textsuperscript{61}, not a first instance. Nor does it have the resources to act as a first instance.

The necessity of an individual assessment in the first instance is also pinpointed by the Board in the case PVN 2009/20: “The Board has tried to map the facts and follow up the claimant with questions, but observes that the claimant has a need for more guidance, clarification of terms and investigation.” It was sent back to the Authority for more clarification due to the consideration for the claimant. The functioning of the two-body structure provides good reasons for requiring the Authority to make some form of individual assessments in line with their role as the first instance in the administrative system.

Another angle is the principle of loyalty enshrined in Article 3 of the EEA Agreement\textsuperscript{62}. The principle of loyalty requires the Member States, including administrative agencies\textsuperscript{63}, to implement EU and EEA law effectively on a national level\textsuperscript{64}. Considering the fact that the Authority is responsible for ensuring an effective implementation of the GDPR on a national level, one could argue that the Authority would fail at ensuring an effective implementation and thus fail to comply with the principle of loyalty if claimants would be left without having their rights established in the individual case. This responsibility is also on the granting authority\textsuperscript{65}.

\textsuperscript{61} Cf. section 22(2) of the Personal Data Act 2018
\textsuperscript{62} Eriksen and Fredriksen (2019) page 51
\textsuperscript{63} Ibid. page 51
\textsuperscript{64} Ibid.
\textsuperscript{65} Eriksen and Fredriksen (2019) page 63
The principle of loyalty requires a highly complex elaboration that falls outside the scope of this thesis. It is however worth mentioning in relation to the interpretation of the clarification duty.

To conclude, the clarification duty in section 17(1) seen together with Article 57(1) GDPR and the consideration for available resources support both answers. Contrary to this, is the existence of a clarification duty in itself and the fundamental two-body structure that arguably require an individual assessment in the first instance. The principle of loyalty in the EEA Agreement may also require an individual assessment in all cases insofar as this is required to ensure an effective implementation of the GDPR.

These arguments lead to the conclusion that the Authority is required to make an individual assessment in all cases which must at least involve a quality check of the material presented by the parties. But the clarification duty cannot be stretched to the point in which the Authority handles a case unjustifiably. At this point, the two-body structure must depart.

### 3.3 Legal positions concerning the Police Databases Act

#### 3.3.1 Explaining the problem

The Police Databases Act is a highly complex legal framework that depends upon a detailed understanding of how the police processes personal data. The act has presented challenges for both the Authority and the Board. As for the Authority’s enforcement of the Police Databases Act, there is especially one interesting case, PVN 2018/17.\(^{66}\)

The respective data subject (“A”) was repeatedly stopped by civil police cars. In one of these controls he was required to perform a blood and urine test. He eventually became curious as to why he was repeatedly stopped for traffic control, and requested the police for access to the data processed on him in the Police log.

---

\(^{66}\) The challenges relating to the Board’s enforcement of the Police Databases Act will be elaborated under section 4.4.
He discovered that there was information entailing that his license was confiscated for three weeks after one of the traffic controls, when it was in fact confiscated for a day. His records further listed “suspicious use of medication”. The police had registered his medical data revealing that he had cancer, that he used Viagra and that there was THC and benzodiazepines in his blood found during a blood and urine test.

“A” requested that the medical data was deleted from the Police log. He also requested the data relating to the confiscation of his license rectified.

After the Police had denied “A”’s erasure and rectification requests on several levels, “A” brought the case to the Authority.

### 3.3.2 The Authority’s competence relating to the Police Databases Act

The Authority has a responsibility to oversee that “the Act and regulations made pursuant to the Act are complied with, and that errors or deficiencies are rectified” cf. The Police Databases Act section 58. This includes to “check that the data relating to the person concerned have been processed in accordance with the Act” upon request from the data subject. If the Authority finds that the processing violates the Act, they may (i) issue a reprimand or (ii) issue an order, cf. section 60. Which of the two options they may use depends on whether or not the processing is connected with an individual criminal case.

### 3.3.3 Procedural elements in the case PVN 2018/17

There is reason to question the way in which the Authority handled the case PVN 2018/17. When the Authority received “A”’s complaint, they requested the Police for a statement as to why the police denied “A”’s claims. The Authority included the rectification claim in their letter to the police, but excluded it from the list of what they “especially” wanted the police to answer at the

---

67 Cf. section 59(1) of the Police Databases Act
68 Ibid. section 60(1) and (2)
end of the letter\textsuperscript{69}. Following this, the police did not explain why they denied “A”’s rectification claim in their response to the Authority\textsuperscript{70}.

Subsequently, the Authority left the rectification claim out of their assessment of “A”’s complaint\textsuperscript{71}. As a consequence, “A” was not given a response as to why the Authority in reality denied his rectification.

This procedure is arguably in violation of the Authority’s clarification duty\textsuperscript{72}. As explained in section 3.2.2, Bernt claims that the clarification duty requires the Authority to make an assessment of the material presented by the parties. This includes “A”’s rectification claim and his explanation of why the license-related material is inaccurate.

This procedure might also be in violation of the claimant’s right to grounds for the individual decision cf. sections 24(1) and 25 of the Public Administration Act. This is especially important where the appellant has been denied a certain claim\textsuperscript{73}.

The Authority’s legal position relating to “A”’s rectification claim is not exactly clear, as they did not have one, despite “A”’s claim. As such, this is not criticism directed to the Authority’s legal position, but to the lack thereof.

It may seem that the appellant’s claim is not necessarily the basis of the Authority’s decision making. In this case, it rather seems as though the response from the police was the basis for the Authority’s decision and that their focus was accepting or disproving the police’s assessments. This could provide a basis for the Authority to review their routines.

\textsuperscript{69} Letter from the Authority to the National Criminal Investigation Service dated 13.07.2017
\textsuperscript{70} Letter from the National Criminal Investigation Service to the Authority dated 01.09.2017
\textsuperscript{71} Letter from the Authority to the claimant dated 21.12.2017
\textsuperscript{72} Cf. section 17(1) of the Public Administration Act
\textsuperscript{73} Eckhoff (2018) page 287
3.3.4 Material elements of the case PVN 2018/17 - should the Authority have reacted to the Police’s processing?

The question of whether or not the Authority should have reacted to the police’s processing in the case PVN 2018/17 is not about the rectification request. However blameworthy the Authority’s case management was in that regard, the rectification request was indeed correctly denied by the Police. This section is rather about the Police’s denial of “A”’s request to delete data relating to his medication. As already mentioned, the Authority shall react to the police’s processing activities if they find it in violation of the applicable framework. Whether or not this entails issuing an order or a reprimand is further elaborated in section 4.3.1.1.

Should the Authority have reacted to the police’s processing of data on “A”’s medication and health condition?

The legal basis for erasing data in the Police log (“politioperativt register”) is section 53-15 in the Police Databases Regulation. Section 53-15 states that sections 50 and 51 of the Police Databases Act and chapter 16 of the Regulation applies. What does chapter 16 of the Regulation and sections 50 and 51 of the Act require?

Section 16-3 of the Regulation states that “personal data…shall be erased when the purpose of the processing has been fulfilled.” Section 50 of the Act states that “Data shall not be stored any longer than is necessary for the purpose of the processing.”

The determinative question is therefore whether or not the storage of “A”’s data on his medication and health is necessary for the purposes of which they were collected.

The reason for this is that the data registered on the driver’s license (“Drivers’ license is withheld until the test results are ready.”), cf. letter to the claimant from the National Police Directorate dated 01.02.2017 page 2, was correct at the time it was registered. It is therefore “accurate” according to section 14-2(2) no. 1 cf. no. 4 of the Police Databases Regulation. This is supported by Ot.prp.nr.108 (2008-2009) page 296-297.
As for the purposes the data was collected for, the general purpose of registering the data in the police log is to have a “continuous overview of all significant data relating to the organization and performance of police services at the site in question”\textsuperscript{75}. The purpose of the Police Database is further elaborated in section 53-6 cf. 53-1, in which data may be registered in the Police log in order to “ensure notoriety of relevant events”\textsuperscript{76} and the “execution of the police operative services”\textsuperscript{77}.

As for the necessity assessment, the relevant data reveals “A”’s health condition meaning that it is special category data cf. section 7 of the Act. Processing of special category data shall only take place if “strictly necessary for the purpose of the processing”\textsuperscript{78}. Processing is “strictly necessary” if it is the “only way of fulfilling the purpose of the processing”\textsuperscript{79}.

The question of whether or not the police should have deleted “A”’s data relating to his medication and health, thus requiring the Authority to react, therefore depends upon whether or not processing “A”’s medication and health data was the only way of fulfilling the purpose of notoriety and execution of the police operative services.

The National Police Directorate was of the opinion that the relevant processing was necessary in order to ensure notoriety of events where the Police has asked that the subject agreed to testing. They further stated that such notoriety is important in order to ensure that the data collectively gives an accurate picture of the police’s task management and interventions towards citizens.\textsuperscript{80}

It is questionable whether or not the registered medical data on “A” was “strictly necessary” for the execution of the traffic control being the relevant police operative services in this regard\textsuperscript{81}. This may constitute grounds for erasing the relevant data.

\textsuperscript{75} Cf. section 10 of the Police Databases Act
\textsuperscript{76} Cf. section 53-1 no. 2 of the Police Databases Regulation
\textsuperscript{77} Ibid. section 53-1 no. 3
\textsuperscript{78} Cf. section 7 of the Police Databases Act
\textsuperscript{79} Cf. section 4-3 of the Police Databases Regulation
\textsuperscript{80} Letter from the National Police Directorate to the claimant dated 12.10.2016.
\textsuperscript{81} Cf. section 53-1 no. 3 of the Police Databases Regulation
However, it is difficult to escape the purpose of ensuring notoriety in the police log. In principle, the purpose of notoriety encompasses everything relating to the execution of police operative services. This includes the use of Viagra as a cancer medication, no matter how distant and peripheral this data may seem in the relevant context. The medical data will also in principle be “strictly necessary”, as complete notoriety relating to police operative services is either ensured or not. This leads to the assumption that, in principle, data registered in the police log may as a basis not be erased under the necessity requirement.

Considering the fact that data registered in the police log will be considered necessary to ensure notoriety in the police log, most likely also strictly necessary, the Authority did arguably not have a duty to react to the police’s processing of “A”’s medical data in the case PVN 2018/17.

4 Legal positions acquired by the Privacy Appeals Board

4.1 An introduction to the Privacy Appeals Board

The Board has, just like the Authority, a significant impact on the rights and duties of the parties involved in the case. In addition, the Board has a seemingly precedential effect on data protection matters. The reason for this is that the Board is the higher administrative agency, and the Authority will take account of the Board’s interpretation when assessing similar legal problems. The Board’s precedential effect provides a particularly important reason to put the Board’s legal positions under scrutiny.

The Board’s function is to decide appeals against decisions made by the Authority. Appeals against a legally binding decision made by the supervisory authority is a fundamental right which the data subject has pursuant to Article 78 GDPR.

---

82 Ibid. section 53-1 no. 2
83 The precedential effect is re-enforced by not being bound by the Authority’s assessments cf. section 34 of the Public Administration Act
84 Cf. section 22(3) of the Personal Data Act 2018.
The Board is, alike the Authority, subordinate to the “King”\textsuperscript{85} and the Ministry of Local Government and Modernisation\textsuperscript{86}. It cannot be instructed about the proceedings in cases or the general day-to-day operations, and the government nor the ministry may overturn their decisions\textsuperscript{87}. The Board is therefore also an independent administrative body.

The Board is a collegiate body with seven members chosen by the “King”\textsuperscript{88}, including a chairman and a deputy chairman\textsuperscript{89}. They have monthly meetings\textsuperscript{90}, in which they handle cases that have been prepared by the secretariat\textsuperscript{91} beforehand. The Board is not bound by the Authority’s factual\textsuperscript{92} or legal assessments\textsuperscript{93}. The decisions are finalized in the meetings. The extent of the prior preparations vary between the different Board compositions\textsuperscript{94} dependent on what they have agreed upon internally\textsuperscript{95}.

\textsuperscript{85} Meaning the government
\textsuperscript{86} Cf. section 22(1) of the Personal Data Act 2018
\textsuperscript{87} Ibid.
\textsuperscript{88} Ibid. section 22(3)
\textsuperscript{89} Ibid.
\textsuperscript{90} The meeting frequency may vary, but according to The Privacy Appeals Board’s yearly reports, for example from 2018 on page 6, they meet ca. once a month.
\textsuperscript{91} Section 3 of the Personal Data Regulation
\textsuperscript{92} The Board shall “try all aspects of the case” cf. section 34(2) of the Public Administration Act
\textsuperscript{93} The Board is “not…bound by the fact that the subordinate instance has considered the conditions to have been fulfilled” cf. section 34(1) of the Public Administration Act
\textsuperscript{94} One Board composition is for example the Board members elected for the period 2017 to 2021.
\textsuperscript{95} This is confirmed by the current chairman of the Board in a personal meeting October 23\textsuperscript{rd}
4.2 Disagreements between the Authority and the Board

4.2.1 Explaining the problem

Since the Board was established in 2001, they have decided a total of 272 cases. The Board disagreed with the Authority’s legal interpretations and final conclusions in 38 percent of the cases between 2006-2019.

A high disagreement rate shows first of all that many areas of data protection law are problematic in a de lege lata perspective. It may be difficult for private individuals, public institutions and

---

96 As per 29.11.2019

97 The disagreement is defined as when the Board reaches another conclusion than the Authority either partly or wholly. The numbers are based on the Board’s yearly report from 2018 on page 7 for the years between 2013-2018 and independent research between 2006-2012 and 2019. Before 2006 there was not consistent date marking in the Board’s decisions. The year 2019 is updated as per 29.11.2019.

98 The total amount of cases handled by the Board in the years 2006 to 2019 are:

2006: 16
2007: 13
2008: 8
2009: 15
2010: 14
2011: 12
2012: 22
2013: 14
private corporations to ascertain their legal positions. Secondly, it proves a need for a compound assessment taking into account all of the presented arguments, as well as possibly relevant arguments left out of the assessments.

The cases provided below are both related to the old data protection framework\(^99\) and the currently applicable framework\(^100\). The relevant legal concepts have not changed much\(^101\), making the agencies’ interpretations relating to the old applicable framework relevant also today, and vice versa to a certain degree.

4.2.2 Legal positions concerning the processing of data relating to criminal convictions

Data relating to criminal convictions represent an especially big threat to the data subject’s privacy, similar to for example data on the subject’s ethnic origin or health. That is why data relating to criminal convictions are, and have been, considered special category data subject to stricter requirements for processing.

Pursuant to section 2(1) no. 8 b) in the Personal Data Act 2000, special category data is “information relating to the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act”. Pursuant to section 11(1) of the Personal Data Act 2018, processing of “data relating to criminal convictions and offences or related security measures” must have a legal basis in Article 9 relating to special category data\(^102\).

---

\(^99\) The Personal Data Act 2000 and the EU Data Protection Directive
\(^100\) The GDPR cf. section 1 of the Personal Data Act 2018
\(^101\) The biggest change is that the Parliament used to elect chairman and deputy chairman cf. section 43(2) of the Personal Data Act 2000. Now, the “King” elects all members cf. section 22(3) of the Personal Data Act 2018.
\(^102\) The applicable legal basis is Article 9(2) a) and c) to f), cf. section 11(1) of the Personal Data Act 2018
The following cases give an impression that neither the Authority not the Board have sufficiently respected the strict requirements for processing data relating to data on criminal convictions. Further, all cases relate to requests for erasing search results from Google\textsuperscript{103}.

In the case PVN 2015/06, “A” wanted all search results on his name removed from Google. Some of the search results linked to news articles elaborating a murder case that “A” was involved in. The articles included his name, portrait photo and the details of his criminal actions. The Authority stated that section 8 f was the applicable legal basis for processing. The reason was that the Google Spain judgement established that Article 6(1) f) was the correct legal basis for de-indexing search results from Google\textsuperscript{104}, and that section 9 did not allow a balancing test between freedom of expression and the data subject’s privacy.

The Board concluded that the relevant data was special category data cf. the Personal Data Act 2000 section 2 no. 8, and that the Authority should have assessed the case pursuant to section 9 relating to the processing of special category data. The case was sent back to the Authority, which again concluded that section 8 f) was the correct legal basis and not section 9\textsuperscript{105}.

In the case PVN 2016/10, there was an article listing persons found guilty, charged or suspected of sexual offences. A Google search on “A”’s name lead to the article, where his actions were described under his name. He wanted the search result removed from the search results on his name. The Authority concluded that this was special category data cf. section 2 no. 8, and that the legal basis for processing was section 8 f) in line with both of their decisions relating to the case PVN 2015/06.

The Board agreed that this was special category data cf. section 2 no. 8, alongside other arguments in the same direction, but stated that the correct legal basis was section 9. They further stated that a strict interpretation of section 9 could not be the legislator’s intention, and that section 9 therefore

\textsuperscript{103} It is important to pinpoint that erasure requests directed towards Google search results in deindexing the relevant search hit, not erasing the relevant information from the source that published the relevant material.

\textsuperscript{104} C-131/12 Google Spain para 73 and 74

\textsuperscript{105} This can be read from the Authority’s statements relating to PVN 2016/10
allowed a balancing of interests between the data subject’s right to privacy versus freedom of expression and the public’s right to information.

In the case PVN-2017-17, DN.no (a newspaper) had published two articles describing “A”’s financial crimes. The first was a judgement where “A” was found guilty of breach of financial trust and complicity to giving the Police an inaccurate explanation. In the second, “A” was found not guilty of breach of financial interest, but sentenced to paying a fine of NOK 10 000 for giving a public authority an inaccurate explanation. “A” wanted Google to erase the two search results under his name.

The Authority and the Board agreed that this was processing of special category data, and that the lawfulness of this processing required a balancing of interests between the freedom of expression and information versus the data subject’s privacy in line with section 8 f), but where the threshold for lawful processing was higher in line with the threshold in section 9.

In a recent case PVN 2019/02, E24.no (also a newspaper) and DN.no had published articles relating to “A”’s convictions on complicity in fraud and gross negligent fraud. “A” wanted Google to erase these search results from his name. The Authority in essence maintained their position from the previous cases, in which the lawfulness of processing required a balancing test between the freedom of expression and information versus the data protection. The Board’s position will be further elaborated below in section 4.2.2.3.

To summarize, the Authority and the Board disagreed on whether or not section 8(1) f) or section 9 was the correct legal basis for processing special category data. They eventually agreed on the character of the assessment, which was that a balancing test between the freedom of expression and information versus data protection was required, although with a higher threshold in line with section 9. Is section 8(1) f) or section 9 the correct legal basis for processing data relating to criminal actions as special category data? And may this processing be assessed on the basis of a balancing test between the freedom of expression and information versus data protection?
Furthermore, in the case PVN 2019/02, the Board suggested that the data subject could be denied his or her erasure request in spite of Google not having a legal basis for processing in Articles 9 and 10 GDPR cf. section 11 of the Personal Data Act 2018. Is this justifiable?

4.2.2.1 Section 8(1) f or section 9 as a legal basis for processing data relating to criminal convictions as special category data?

First is the disagreement relating to whether or not section 8(1) f) is the accurate legal basis for processing data relating to criminal actions as special category data cf. section 2 no. 8 b).

The Authority referred to the Google Spain decision\textsuperscript{106} when stating that section 8 f) was the correct legal basis in all of the cases mentioned above. Sections 73 and 74 stated that Article 7 f) in the Directive – similar to section 8 f) in the Personal Data Act 2000 and Article 6(1) f) in the GDPR – was the correct legal basis for processing relating to processing “carried out by the operator of a search engine”.

Firstly, the court in the Google Spain case did not establish that the relevant data was special category data, contrary to what the Authority concluded in the relevant case. The transfer value of the judgement is therefore limited. This was also the Board’s argument in the case PVN 2019/02.

Secondly, section 9 regulates the processing of special category data specifically. Paragraph one reads as follows: “Special category data may only be processed if the processing fulfils the requirements in section 8 and (section 9 a) to h))”. Section 8 is therefore indeed a legal basis for processing the relevant data, but this data cannot be found lawful without assessing section 9, contrary to what the Authority did.

4.2.2.2 Processing of special category data based on a balancing test between freedom of expression and information versus data protection?

Second is the solution that the Authority and the Board more or less agreed on in the first three cases. This solution was that lawful processing of data required a balancing test between freedom

\textsuperscript{106} C-131/17 para 73 and 74
of expression and information versus data protection in line with section 8(1) f). The balancing test was performed in light of a higher threshold adjusted to the sensitive nature of the data in line with section 9.

The Authority and the Board in essence interprets section 9 to allow processing for the purposes of freedom of expression and information. This is peculiar considering the fact that section 9 does not allow processing for the purposes of freedom of expression and information. Section 9 derives several balancing tests, but only for the following purposes: “vital interests”\textsuperscript{107}, “establishment, exercise or defense of a legal claim”\textsuperscript{108}, “to enable the controller to fulfil his obligations or exercise his rights in the field of employment law”\textsuperscript{109}, “the purposes of preventive medicine” etc.\textsuperscript{110} and “historical, statistical or scientific purposes, and the public interest…”\textsuperscript{111}.

The Authority referred to the right to object to processing cf. Article 14(1) of the Directive in support of their position that processing special category data required a balancing test between the data subject’s privacy and freedom of expression and information. Section 8(1) f) was indeed a relevant assessment relating to the data subject’s right to object to processing\textsuperscript{112}. This reference was however made before the Authority had concluded on the question of legal basis for processing in sections 8 and 9 cf. section 11.\textsuperscript{113}

The method in data protection law is that one must always assess a legal basis for processing before assessing the data subjects’ rights\textsuperscript{114}. If Google does not have a legal basis for processing in section 9, one cannot legalize their processing because the data subject did not fulfil the requirements for the right to object to processing under Article 14(1) a). The right to object cannot therefore be used

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{107}] Cf. section 9(1) c) of the Personal Data Act 2000
\item[\textsuperscript{108}] Ibid. section 9(1) e)
\item[\textsuperscript{109}] Ibid. section 9(1) f)
\item[\textsuperscript{110}] Ibid. section 9(1) g)
\item[\textsuperscript{111}] Ibid. section 9(1) h)
\item[\textsuperscript{112}] Ot.prp.nr.92 (1998-1999) section 5.4.1.3 and 5.4.1.5 entails that the right to object to processing cf. Article 14(1) is applicable in Norwegian law even though it was not expressly included in the Personal Data Act 2000.
\item[\textsuperscript{113}] See PVN 2015/06
\item[\textsuperscript{114}] Cf. section 11(1) a) of the Personal Data Act 2000
\end{itemize}
\end{footnotesize}
to allow processing of special category data for the purposes of freedom of expression and information which would not be permitted pursuant to Articles 9 and 10.

The Board referred to the preparatory works in support of their position, and further that this position was in line with Norway’s international obligations and the protection of civil and political human rights enshrined in the Constitution.\footnote{PVN 2017/17}

As for the international obligations and the Constitution, these arguments have not been commented further by the Board, and will therefore be difficult to try.

The preparatory works stated that section 9 was meant to “carry forward and elaborate the necessity requirement in the Personal Data Filing System Act 1978”. This is a very general comment and may hardly constitute an argument to allow processing for other purposes than those listed. It must also be mentioned that section 9 holds five necessity requirements, but not for the purposes of freedom of expression and information.

Furthermore, the same preparatory works also state that section 9 gives an exhaustive list of legal bases for processing special category data\footnote{NOU 1997:19 page 139 and Ot.prp.nr.92 (1998-1999) page 110}. This is a rather clear statement. It also supports the natural meaning of “may only be processed if (...)” in section 9(1).

The fact that the preparatory works mention a general purpose to carry forward the necessity requirement in the Personal Data Filing System Act is not a strong enough argument to contradict the wording of section 9 and the preparatory works reinforcing the exhaustive nature of section 9.

One could suggest that section 7, which allows all processing for the purpose of freedom of expression, thereunder for journalistic purposes, could allow Google’s processing of the relevant news articles. However, section 7 does not apply to Google as Google itself does not have journalistic purposes for indexing search results contrary to the newspapers that published the relevant articles.
Allowing the processing of special category data for the purposes of freedom of expression and information would entail a lower degree of protection than section 9 entails, thus making the added protection of section 9 illusory.

The conclusion is that data relating to criminal convictions is considered special category data cf. section 2(1) a) which must be assessed pursuant to sections 8 and 9. If Google does not fulfil the requirements set out in section 9, they do not have a legal basis for processing.

4.2.2.3 No need to establish a legal basis for processing?
Third is the Board’s position in the case PVN 2019/02. The Board held that a balancing test between the freedom of expression and information versus data protection was required. Their approach was nevertheless different to the three first cases, as this case was assessed pursuant to the GDPR.

The Board claimed that it was not necessary to conclude on whether or not there was a legal basis for processing in this regard. This was supposedly supported by the CNIL judgement117, which they claimed to support a view in which the data subject could not be afforded the right to erasure in spite of a lacking legal basis for processing if the consideration for freedom of expression outweighed the data subject’s privacy. It was also supported by Article 17(3), which they claimed gave Google a right to deny erasure if the processing was necessary for the purpose of freedom of expression and information.

As for the CNIL judgement, the court indeed stated that de-indexing search results must be assessed in light of Article 11 of the ECHR affording individuals a right to information. However, the Norwegian legislator has chosen to make national adjustments in line with Article 10, in section 11 of the Personal Data Act 2018. According to section 11, data relating to criminal actions may only be processed if there is a legal basis in Article 9(2) a) and c) to f). The court in the CNIL

117 C-136/17 G.C. and Others v CNIL
judgement did not take account of Norwegian adjustments in this area. Further, the EU court cannot override clear national legislation.

As for Article 17(3) allowing Google to deny an erasure request, the method in data protection law requires establishing that the processing is lawful before attending to the data subject’s rights. One cannot use the assessment required in relation to the subject’s rights in Chapter III GDPR to assess the general lawfulness of processing. This is especially so considering the fact that the provisions relating to data subjects’ rights do not mention special category data.

In conclusion, the Board has arguably undermined the significance of section 11 of the Personal Data Act 2018 and Articles 9 and 10 GDPR when establishing that there is no need to conclude on the legal basis for processing under the GDPR because of the right to freedom of information enshrined in Article 11 ECHR and the CNIL judgement. The assessment should have been based in Articles 9 and 10 GDPR cf. section 11 of the Personal Data Act 2018.

4.2.3 Legal positions concerning the scope of consent
Another source of repeated disagreement is the scope of consent. This disagreement relates more specifically to the following case types:

- Whether or not the original consent relating to a health research project is valid also for an extended health research project
- Whether or not parents’ consent on behalf of their children is valid after the children become 16 years of age

4.2.3.1 The scope of consent relating to health research projects
There are two cases worth mentioning in this regard: PVN 2013/14 and PVN 2018/03. It is difficult to make a general assessment on the basis of both decisions due to the difference in the cases’ facts. The assessments of the Authority’s and the Board’s legal positions will therefore be connected to each case.
In the case PVN 2013/14, the purpose of the original research project “Farmer’s biobank” was originally to “map allergy, airway and lung diseases in agriculture” connected with dust in light of production type and work methods. The processing was based on consent. Statens Arbeidsmiljøinstitutt later wanted to use the same data to make a thematic research registry for national and international use to research exposures relevant for “health issues, sickness and death” amongst farmers, including cancer, and transfer the data to the Cancer Registry of Norway. This without retrieving new consents.

The Authority claimed that the original consent covers only the original purposes, i.e. processing regarding dust related disease, and was not valid relating to the expanded project, cf. section 2 no. 11 of the Personal Health Data Filing System Act 2001. The Board disagreed, and claimed that the original consent covered also the expanded project cf. section 2 no. 11.

Should Statens Arbeidsmiljøinstitutt have retrieved new consents relating to the extended health research project?

The Authority’s conclusion is based on the perception that the expanded project involved a considerable change of purposes, in which the relevant health conditions were made more comprehensive, and that the extended project transferred the controllership from STAMI to the National Cancer Registry. It was also mentioned that the extended project involved the establishment of a scientific research registry, which was not in line with the original health research form.

The Board was of the opinion that there was a causal relationship between the original and the extended purposes. The consent therefore covered the extended purposes. The differences in purposes were “allergy, airway and lung diseases” relating to dust versus “health issues, sickness and death”.

An expansion of which health conditions are taken into the research is arguably information the data subject should be aware of relating to his or her consent. This could entail that the criterion
of an “informed” consent\textsuperscript{118} is not fulfilled, and that the original consent is not valid relating to the extended project.

On the other hand, the data subjects were given information explaining that the research was aimed at understanding different diseases occurring with farmers. This is work that does not exactly have a specific time limit, and indicates a vast variety of relevant health conditions. Also, the character remains more or less the same: farmers’ health conditions. This could entail that the subjects’ consents would be sufficiently “informed” also relating to the extended project.

As for the establishment of the new registry itself, this does not necessarily constitute a game changer relating to the original project. All research projects require some form of registry to maintain a systematic overview of the relevant data. It is difficult to see how the original project did not involve an organized registry. The new registry is however less ad hoc-based than the original and is aimed specifically on future research. But this should not be considered different to the degree where the original consent is not valid.

Also, scientific research is a wanted processing activity in order to be effective. The GDPR acknowledges that “It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection.”, and that consents may take account of this.\textsuperscript{119}

Therefore, there are good reasons for stating that as long as one maintains the character of the original purposes, which was studies on farmers’ health conditions, one must sometimes accept a considerable extension of the scope of these purposes due to the unpredictable nature of research and the public benefits of scientific research.

But the extended project also involved a transfer of controllership from STAMI to the National Cancer Registry. This is more problematic for the validness of the consent. The Personal Data Act

\textsuperscript{118} Cf. Section 2 no. 11 of the Personal Health Data Filing System Act
\textsuperscript{119} Recital 33 GDPR
2000 and the Data Protection were silent as to whether or not a valid consent presupposes information on the identity of the controller.

But the Working Party 29’s guidelines on consent stated that for a consent to be “informed”, the data subject must be provided with the necessary information, which “would normally cover the elements of information listed in Article 10 of the Directive.”\textsuperscript{120} Article 10 requires the controller to give information on “the identity of the controller” cf. Article 10(2) a). Without requiring new consents, there would be no way of ensuring that the data subjects were informed of the change of controllership of their data. The original consent would therefore most likely not be “informed” as the data subjects would not be familiarized with the controller’s identity.

To conclude relating to the case PVN 2013/14, Statens Arbeidsmiljøinstitutt would most likely be required to retrieve new consents from the data subjects involved in the original research project contrary to the Board’s position. This is due to the fact that the extended project involved a transfer of controllership combined with the fact that an “informed” consent requires information on the controller’s identity.

In the case PVN 2018/03, Folkehelseinstituttet had together with the University of Oslo and Ullevål Universitetssykehus established the Norwegian Twin Registry. The question was whether or not the data subjects had consented to processing of their data in the Twin Registry. There were three types of data sets in question: 1) inclusion of dead twins, 2) inclusion of data from the study “Health problems, personality and life quality and 3) inclusion of data from the study “Psychological disorders relating to twins – a follow-up study”.

The Authority and the Board disagreed on the two first data sets, based on respectively an interpretation of section 2 no. 11 of the Personal Health Data Filing System Act of 2014 and Article 4(11) GDPR.\textsuperscript{121} The discussion relating to the inclusion of dead twins is the most interesting aspect

\textsuperscript{120} Working Party 29 Opinion 15/2011 page 9

\textsuperscript{121} The main difference between the two frameworks is that the GDPR requires a clearer affirmation of consent than the Personal Health Data Filing System Act of 2014.
relating to the Authority’s and the Board’s legal positions relating to the enforcement of data protection law.

As for the inclusion of dead twins, it seems as though the Authority did not consider the fact that dead people are not protected by the Personal Data Act cf. section 2 no. 1, when stating that “all registration in the Norwegian Twin Registry must be based on consent”. This lead to the conclusion that data on the dead twins could not be included in the registry.

The Board pointed out that inclusion of dead twins is permitted when the living twin consents, because a dead twin is only protected under the GDPR (and the Personal Data Act of 2000\textsuperscript{122} for that matter) insofar as their data can be connected with the living twin\textsuperscript{123}. This leads to the assumption that the inclusion of the dead twins should have been permitted by the Authority.

4.2.3.2 Parents’ consent on behalf of their children
The Authority and the Board have further disagreed on whether or not parents’ consent on behalf of their children is valid when the child becomes 16 years of age and allowed to consent on his or her own.

In the case PVN 2013/07, the registry “Norsk Nyrebiopsiregister” processed children’s personal data based on their parents’ consent on behalf of their children. The Authority concluded that the registry was required to collect consents from the children when they turned 16. The Board claimed that the consent was valid beyond the age of 16, at which point the right to withdraw the consent transfers to the teenager. The Board’s conclusion presupposed that the processing purposes did not change. Both assessments were pursuant to section 2 no. 11 of the Personal Health Data Filing System Act of 2001.

\textsuperscript{122} Section 1 of the Personal Data Act 2000
\textsuperscript{123} Recital 27 GDPR
In the case PVN 2014/21, the registry “Norsk Brannskaderegister” also processed children’s personal data based on their parents’ consent. The Authority and the Board maintained their conclusions from the previous case\textsuperscript{124}.

The point of disagreement was therefore whether or not a consent that parents give on behalf of their children is valid after the children turn 16.

The preparatory works of the Personal Health Data Filing Act of 2014 state that parents’ consents on behalf of their children is valid after the children turn 16, at which point the child may withdraw their consent\textsuperscript{125}. This was not further explained. The mentioned preparatory works did not apply in the two mentioned cases as these cases were assessed pursuant to the Act of 2001, but it would seem as though the question has been answered for the time being.

However, one might question whether or not this is a good norm. It presents challenges to fundamental elements of a valid consent. This regards in particular the requirement of an “informed indication of the data subject’s wishes” consent. The Authority has also expressed principle views going against this norm.

The Authority expressed that a consent given by a child’s parents will be considered a passive and thus invalid consent when the child turns 16.

In the recent Planet49 case\textsuperscript{126}, the court stated that “the requirement of an “indication” of the data subject’s wishes clearly points to active, rather than passive, behavior. (…) consent given in the form of a preselected tick in a checkbox does not imply active behaviour”.

Even though consent to cookie policies and consents transferring from parents to children are quite different situations, one could argue that the court’s position is relevant also in this case: A data

\textsuperscript{124} The Board based their position on the Personal Health Data Filing System act of 2014, but explained that the new act does not entail any changes in this matter.

\textsuperscript{125} Prop.72 L (2013-2014) page 195

\textsuperscript{126} C-673/17 Verbraucherzentrale Bundesverband eV v Planet49
subject is presented with a situation which requires his or her consent. The consent is not necessarily an “indication of (his or her) wishes” if the subject must make an active move to remove a consent. This leads in the direction that the registry should retrieve the child’s consent after he or she has turned 16.

As for the criterion of an “informed” consent\textsuperscript{127}, the child might not know about the relevant processing when he or she turns 16. The Board also stated in the case PVN 2013/07 that registries were not obliged to inform the subjects of the processing activities or their right to retrieve their consents. How can there be an “informed” consent if the child does not even know about the relevant processing? The parents might die or forget, or other circumstances may prevent this information from reaching the child.

Further, a fundamental thought in data protection law is that a data subject should have control of their data. Regardless of the circumstances in which the parents consented on behalf of their children, these children do not have sufficient control of the relevant consent when they turn 16 in light of the considerations presented in the paragraph above. If the children’s consent must be based solely on the circumstances of the parents’ consent, the child’s rights and consent becomes slightly illusory after the age of 16.

On the other hand, a consent is considered valid until it is withdrawn. This was emphasized by The Board in the mentioned cases. In this way, the fact that a consent swaps owners should not have any effect on the validness of this consent. Also, the validness of a consent is typically assessed on the basis of the circumstances at the time the consent was given. This would entail that a parent’s consent on behalf of their child should remain valid when they turn 16.

There is no clear answer to whether or not a consent given by parents on behalf of their children should be valid after the child turns 16. It is solved in the preparatory works for now. One is faced with the dilemma between the consideration that a consent is valid until it is withdrawn and the fact that fundamental elements of a consent and the notion of control is challenged if the consent

\textsuperscript{127} Cf. section 2 no. 11 of the Personal Health Filing System Act
given on behalf of the child remains valid after it turns 16. A solution which possibly could maintain the fundamental concepts of a valid consent and the child’s control, as well as the registries’ need for processing, is to establish that the parents’ consent is not valid after the child turns 16, at which point the registry must fulfil another legal basis for processing in order to be allowed further processing of the children’s data.

The recent case PVN 2018/05 provides a different legal and factual reality than the two cases mentioned above, creating other legal challenges. The processing in the EILO registry (Exercise Induced Laryngeal Obstruction) was alike the two previous cases based on the parents’ consent, but the consent form expressly stated that the consent would only apply until the child was 16. The Authority and the Board agreed that due to this expressed limitation, the consent was invalid after the child was 16.

The Authority based their conclusion on the definition of consent enshrined in section 2 e) of the Personal Health Data Filing Act 2014, and did not assess other legal bases for processing. The relevant consent would not be an “informed and unambiguous indication of the data subject’s consent”, and the registry was not allowed processing after the children turned 16. The Board concluded that processing the relevant data after the children turned 16 was allowed on the basis of the definition of consent in Article 4(11) GDPR and Articles 6(1) f) and 9(2) j).

Article 9(2) j) is arguably an unfit legal basis for processing of children’s personal data for the purposes of establishing a registry aimed for research.

Article 9(2) j) reads as follows: “processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes”. The Board indeed elaborates on how the registry fulfils the requirement “scientific research purposes”, but does not at any point elaborate the requirement “archiving purposes”.

Archiving is an activity that in a sense presupposes that the relevant data is no longer actively used. If the EILO registry was meant for future research, one could say that the registry falls outside the scope of Article 9(2) j).
In connection with Article 9(2) j), the Board refers to section 9 of the Personal Data Act 2000 and 2018 and the legal basis allowing processing which is “necessary for reasons of substantial public interest”. This legal basis corresponds to Article 9(2) g). The Board subsequently state that “In other words, there must be a balancing of interests pursuant to Article 6 f) and Article 9(2) j), cf. section 8 of the Personal Data Act 2018.

This introduction of the relevant legal basis for processing may be questioned. The Board in essence provides two different legal bases for processing, namely Article 9(2) g) and j) relating to respectively “substantial public interest” and “archiving purposes”, while presenting it as one and the same. The content of the assessment corresponds with “substantial public interest”, while the formal reference is Article 9(2) j) “archiving purposes”.

On one side, the Board performed a thorough assessment of whether or not the EILO registry had a “substantial public interest” for processing the relevant data, and whether or not the subjects’ privacy overrode this interest. This entails that the suggested material mistakes were insignificant in the relevant case.

On the other side, the legal basis for Board’s assessment appears to be somewhat disconnected and is difficult to understand. This is unfortunate considering the fact that the Board’s assessments provide guidance for the Authority’s practice and other data protection practitioners as well. It is important that the Board maintains a transparent and easily understandable practice in order to ensure a transparent application and enforcement of data protection law.

4.2.4 Camera surveillance

The Authority and the Board have disagreed on camera surveillance matters in a number of cases over many years. The disagreement relates to the balancing test required in the assessment of lawful camera surveillance and storage time for surveillance data.

The disagreements between the Authority and the Board must be understood in light of the purposes of the surveillance. The cases in which the agencies have disagreed relate to (i) protection
of property, (ii) public interest of protection of individuals and (iii) detection and prevention of crime.

The cases on camera surveillance were established when the old Personal Data Act from 2000 was applicable. In the old act, Chapter VII established certain rules on when camera surveillance is lawful. These cases are relevant to the interpretation of the currently applicable camera surveillance provisions due to the fact that also these provisions require a balancing test between the purposes of camera surveillance and the data subject’s privacy.\(^{128}\)

### 4.2.4.1 Protection of property

In the case PVN 2002/02, the question was whether or not Posten Norge was allowed to extend the storage time for the surveillance tapes connected to an ATM outside of the building. The Authority claimed that the term “special need” in the Personal Data Regulation\(^{129}\) had to be interpreted strictly, requiring special circumstances for extended storage time. They concluded that Posten did not fulfil the requirements for extended storage time beyond 7 days.

The Board did not agree that “special need” was meant to be interpreted strictly or that there had to be special circumstances. Their position was that “special need” must be interpreted based on a comprehensive assessment of the different considerations applying to extended storage time. They concluded that the criterion was fulfilled, and that Posten was allowed to store the surveillance data for three months.

The assessments made by the Authority and the Board are nuanced and thorough. Both agencies have elaborated on the potential risk relating to the ATM and the relevant privacy concerns to an extensive degree. This case shows that the question of lawful camera surveillance is highly complex and may not have a given answer based on the surrounding sources of law.

In the case PVN 2013/03, the question was whether a goldsmith had a right to continuously surveil the area behind the counter where the employees were, and the customer area. The purpose was to

---

\(^{128}\) Especially Article 6(1) f) «legitimate interest» and e) «public interest»

\(^{129}\) Section 8-4(2) of the Personal Data Regulation
more easily solve or prevent robberies and burglaries, and to surveil the valuables in the store. Both the Authority and the Board interpreted section 38 (the criterion “special need”) of the Personal Data Act of 2000.

The Authority did not accept the goldsmith’s argument that surveillance of the mid-area behind the counter, in between the break room and the customer area, was necessary due to a risk of robberies and burglary. They also stressed that a continuous surveillance of staff areas required especially compelling reasons.

The Board disagreed, and concluded that the camera surveillance fulfilled a “special need”. The reason for this was that the surveillance was limited to the areas where easily tradable valuables were handled with an increased risk of criminal offences, and that the break room was not surveilled. The goldsmith also outsourced the surveillance and storage to an external security company, removing the possibility of monitoring the employees’ work. Further, the employees were informed of the surveillance prior to their employment, meaning that their data protection rights were sufficiently maintained.

In this case, the goldsmith arguably fulfilled a sufficient legitimate interest for surveilling the mid-area because this area had valuables and was therefore a target for robberies. At the same time, the risk of monitoring employees may be considered to be removed by outsourcing the surveillance.

However, the EDPB\textsuperscript{130} has stated that “The legitimate interest needs to be of real existence and has to be a present issue…It is…not sufficient to present national or general crime statistic without analyzing the area in question or the dangers for this specific shop.”\textsuperscript{131} The EDPB mentions jewelers as an example of “imminent danger situations (that) may constitute a legitimate interest”\textsuperscript{132}.

\textsuperscript{130} European Data Protection Board Guidelines 3/2019. Page 5. The EDPB’s work relates to the GDPR, but the provisions are not noteworthy different and the guidelines may therefore be used to assess the cases under the old framework.

\textsuperscript{131} EDPB Guidelines 3/2019 page 8

\textsuperscript{132} Ibid. page 8
A potential weakness with the Authority’s and the Board’s assessments is that both agencies connect the purpose of camera surveillance, i.e. solving and preventing robberies, to a more general crime picture relating to all goldsmiths. One could argue that in light of the EDPB Guidelines, the assessment of the crime picture should have been more connected with a proven risk of robberies in this specific store and/ or town rather than goldsmiths in general.

In the case PVN 2016/01, NorgesGruppen wanted to extend storage time for surveillance data connected with bank in stores solutions (“Bank i Butikk”). The purpose was to solve and prevent cases of embezzlement from the employees. The Authority and the Board interpreted “legitimate reason” in the Personal Data Regulation section 8-4 (6). They agreed that extended storage time for the surveillance tapes overlooking the entrance area was not lawful, but disagreed on the tapes overlooking the cash safe in the store. The Authority denied processing overlooking the cash safe, while the Board allowed it.

The Authority’s position was based on the view that the embezzlement was limited in scope, and that the surveillance was a violation of the employees’ integrity and a sign of distrust. The Board’s conclusion was based on the perception that surveillance monitoring only the person opening and closing the safe was not a particular violation against the employees’ integrity. Also, the surveillance did not overlook the customers.

In this case, the Board did not seem to consider the principle privacy concerns that surveillance of employees entails. They simply established that this surveillance is not particularly problematic relating to the employees’ integrity without further comment. The conclusion in favor of extended storage time was based on a “discretional balancing test” (“skjønnsmessig avveining”), without elaborating on the actual balancing exercise. The Board’s assessment is arguably too thin in this matter, especially considering the fact that they reversed the Authority’s decision on this point.

Based on these three cases, it seems that (i) the Board seemingly requires less of what needs to be proven relating to risk than the Authority and (ii) the Authority is more skeptical relating to surveillance of employees on a principle level than the Board. The Authority’s and the Board’s assessments will possibly be more alike and comparable in the future in light of more detailed
guidelines from the EDPB on the matter than what the Working Party 29 provided at the time of these cases.

4.2.4.2 Public interest or protection of individuals

In the case PVN 2005/13, the question was whether or not NSB could surveil their trains, hereunder the area surrounding the driver passenger compartments. The purpose was to ensure the employees’ and the passengers’ security. The Authority concluded that NSB were not allowed to surveil the compartments. The Board disagreed, and constituted that surveillance of the compartments was lawful.

The Authority based their decision on the fact that the purpose of the surveillance was possible through a more limited surveillance which only covered the entrance areas, cf. section 8 f) of the Personal Data Act of 2000. The Board based their conclusion on the possible preventive effect of the surveillance cameras and the possibilities for supplementing facts connected to potential violent episodes. This was sufficient pursuant to section 37(1) cf. section 8 f).

In addition to disagreeing on the conclusions in the case, the agencies also disagreed on which elements were relevant in the individual assessment. The Authority stated that signage and information could not be relevant in the assessment as these are in fact legal requirements in the case of camera surveillance, while the Board held that this was a relevant element, without further comment. Adding to this, the Authority stated that the more general level of camera surveillance in the society was relevant as this perspective prevented the assessments from losing perspective, while the Board stated that the law required an individual assessment, in which general societal considerations were irrelevant.

When trying to understand the core of the disagreement in this case, it seems as though the Authority and the Board disagree on 1) whether or not camera surveillance in compartments is privacy-intrusive on the passengers, and 2) what NSB needs to prove in order to establish a legitimate interest overriding the privacy considerations.
As for the first element, the Authority stated that passengers expect discretion, while the Board considered compartments as a very public area where passengers should expect to be observed.

As for the second element, the Authority required NSB to prove that a less privacy intrusive solution, i.e. surveillance of the entrance areas only, would not be sufficient for the preventive effect and finding the responsible people behind violence and vandalism, before the Authority could allow compartment surveillance. The Board did not focus on the fact that camera surveillance is generally not permitted if a less privacy-intrusive solution suffices. They rather concluded that a “possible” preventive effect and the “possibility” for detailed information on violence episodes was sufficient.

The latter arguments were based on statistics from two Danish articles relating to Danish territory, and an assumed psychological effect. One cannot automatically assume that behavior in one country applies in another. The Board has in fact stated that research from other countries is a weak source\(^\text{133}\). In addition, the potential psychological effect should have been based on documented research.

The preparatory works stated that “a possibility” that the surveillance may help the legitimate need of the controller is not enough\(^\text{134}\). The EDPB has claimed that camera surveillance must be of “real existence and has to be a present issue”, and the legitimate interests must be documented somehow in order to prove that the concerns are not speculative\(^\text{135}\). The Board has arguably based their conclusion on insufficient documentation.

### 4.2.4.3 Detection and prevention of crime

In the case PVN 2005/12, the question was whether or not Sporveisbussene was allowed to have camera surveillance on their buses, hereunder the area surrounding the driver and the passenger area. The purpose of the surveillance was to prevent robberies and violence, which many of the

\(^\text{133}\) PVN 2017/10 “Both the appellant and the Data Protection Authority have referred to reports which have analyzed the preventive effect that camera surveillance actually has. These reports differs, do not relate to Norwegian circumstances, and have thus a very limited significance.”

\(^\text{134}\) Prop.47 L (2011-2012) page 43

drivers had experienced during their shifts. The Authority concluded that Sporveisbussene were only allowed to surveil the drivers’ area, while the Board allowed surveillance of the passenger area as well cf. section 37(1) cf. section 8 f).

The Authority based their conclusion on statistics showing that the majority of threatening events occur around the drivers’ area during ticketing. They also referred to the intrusive character of surveillance in passenger areas of a bus. The Board stated on their end that surveillance in the passenger areas will contribute to a sense of security amongst the passengers. Also, surveillance has a preventive effect on violence, as well as on property damage in the buses.

A questionable element in the Board’s assessment is that their conclusion was based on passenger safety, when there was in fact little proof in the relevant documentation that passenger areas were prone to violence episodes. Preventing and solving violence episodes was after all the purpose of the surveillance. It is important to avoid accepting surveillance in all areas where there is a certain risk of violence or other legitimate interests for surveillance. Such risks must be proven in the individual case, and the privacy-intrusive character of camera surveillance must be respected.

In the case PVN 2017/10, the question was whether or not camera surveillance of certain areas in Brumunddal centrum was lawful. The purpose was to solve and prevent criminal actions in the town centrum. The Authority concluded that the processing was not lawful subject to section 37(1) cf. section 8 f). The Board disagreed, and concluded that the crime scene was significant enough to allow the relevant surveillance.

The Authority based their conclusion on a perception that the crime scene in the centrum was limited, and that the extent of camera surveillance in the central areas was comprehensive (5 cameras covering 12 % of the centrum). The supposedly limited crime picture was due to the fact that the police could only account for a “felt” sense of insecurity, not an actual, documented insecurity.
The Board based their conclusion on a longer time frame underlying the crime assessment, that the Police had already tried other means of handling the crime and that the data processing was limited by access control and a standard storage time of 7 days.

The core of the disagreement in this case was that the Authority and the Board disagreed on the crime scene in the town centrum. The Authority claimed that 13 criminal offences did not constitute “repeated or serious criminal offences” cf. section 37(3). The Board claimed there is no doubt that these events constituted “repeated criminal offences”. The Authority further claimed that the crime scene at the time of the case was not the same as it was during the time period of 2006-2009, when there were especially many fires and violence episodes in Brumunddal. They did not explain why they limited the time frame to the years 2006 to 2009.

The Board claimed that the assessment had to be based on the time period 2006-2014, when the camera surveillance was enacted. After 2006, there was a series of vandalism and violence episodes. The fact that the Police had solved 20 criminal offences based on the surveillance tapes reinforced the legitimacy of the surveillance enacted to prevent and solve criminal offences. Further, the Board pointed out that the Authority did not consider the fact that the Police had already tried patrols, increased manual security and beautification of the centrum – without the desired effect. Nor had they considered a less extensive camera surveillance as an alternative to an absolute prohibition of camera surveillance.

One might argue that the Authority has required too much relating to establishing a necessary crime scene, and has used a time frame that was too short to make a fair assessment of the crime scene in Brumunddal centrum.

4.3 Legal positions concerning the Police Databases Act

On the 12th of August 2019, the Police Department sent an e-mail to the Justice Department asking for their point of view on the Privacy Appeals Board’s interpretation of the Police Databases Act. The Directorate suggested that the Board had misinterpreted certain provisions in the Police
Databases Act, which further suggests that the Board does not sufficiently understand the police’s processing activities. The Justice Department has not yet made a statement in this matter.\(^{136}\)

4.3.1 Section 60(1) and (2) of the Police Databases Act – processing in connection with or not in connection with a criminal case?

4.3.1.1 Explaining the problem
One of the matters the Police Directorate addresses is that the Board has misinterpreted section 60(1) and (2) of the Police Databases Act.\(^{137}\) The Authority has concluded that processing of personal data in the police log may be considered personal data in connection with a criminal case. The Directorate suggests that this practice builds upon a fundamental misunderstanding of how the police processes personal data. Their position is that processing of personal data in the police log shall always be assessed pursuant to the provisions not in connection with a criminal case.

The question of whether or not the processing is considered connected with an individual criminal case or not is important as it is decisive for the Authority’s powers. In the case of processing in connection with a criminal case, the Authority may issue a reprimand.\(^{138}\) The Police should consider the Authority’s reprimands, but is not obliged to comply with them.\(^{139}\) In the case of processing not in connection with a criminal case, the Authority may issue an order which the Police is obliged to comply with.\(^{140}\)

The relevant cases and the Police Directorate’s inquiry to the Justice Department will be elaborated below, before making an assessment of the relevant sources of law.

4.3.1.2 The Directorate’s inquiry
The Directorate wrote the following in their inquiry to the Justice Department from August 12th 2019:

---
\(^{136}\) As of 29th of November 2019
\(^{137}\) Section 60(1) and (2) will be introduced in further detail in section 4.3.1.3
\(^{138}\) Cf. section 60(2) of the Police Databases Act
\(^{139}\) Ot.prp.nr.108 (2008-2009) page 324
\(^{140}\) Cf. section 60(1) of the Police Databases Act
\(^{141}\) Ot.prp.nr.108 (2008-2009) page 324
“The Directorate has interpreted and practiced the framework in the way that the information in the Police Database will be interpreted according to the provisions on processing not in connection with an individual criminal case, independently of whether or not the information is also processed in connection with the criminal case. Otherwise, large amounts of the information in the Police Database will be excluded from the Data Protection Authority’s competence to issue orders, cf. the Police Databases Act section 42-2.” The Directorate herein refers to the cases PVN 2018/17 and PVN 2018/19.

In the case PVN 2018/17142, the Board concluded “there is no doubt that the data was collected and registered in the Police Databases in connection with a criminal case”. This was because the data was collected for the purpose of determining whether or not the driver was driving under influence. Suspicion of driving under influence is regulated in the Criminal Procedure Act sections 1 and 2.

In the case PVN 2018/19, there was data in the Police Database explaining that “A” had been observed drunk on a train in 2009, that “A” had been the victim of rape in June 2014, alongside information of a message of concern from a family member from 2015 explaining “A” had attained a gun, was drunk during weekdays and was on a timely basis paranoid and depressed following the assault.

The Board concluded with processing in connection with a criminal case (the data related to sexual assault) as well as processing not in connection with a criminal case (the message of concern and information about the subject’s drunken appearance on the train). The Authority has not explained why they considered the data related to sexual assault as data in connection with a criminal case.

4.3.1.3 An assessment of section 60(1) and (2)

On the basis of the Directorate’s inquiry to the Justice Department and the Board’s case law, it becomes clear that the Board and the Police Directorate have different perceptions of the correct

142 This case was introduced in section 3.3.1
practice relating to section 60(1) and (2) in the Police Databases Act. The more specific question is whether or not processing in the police log shall be assessed pursuant to the provisions on processing *in connection with* or *not in connection with* a criminal case.

The question of what the correct practice is comes down to an interpretation of the terms “processing of data other than in individual criminal cases” cf. section 60(1), defining the competence to issue an order, and “processing of data in connection with criminal cases” cf. section 60(2), defining the competence to issue a reprimand.

The Board has not elaborated in detail why they consider some personal data as “processing of data in connection with criminal case” cf. section 60(2). The reasoning in the case PVN 2018/17 and a conversation with a representative from the current Board does however lead to the following perception: If personal data is collected in the police log with the purpose of investigating a possible criminal offence, or personal data in the police log is related to a criminal case otherwise, the relevant personal data in the police log is considered “processing of data in connection with a criminal case” cf. section 60(2).

This perception can be explained from a practical interpretation of “in connection with”. If the police needs personal data registered in the police log for a criminal investigation, such as witness names at the scene of a sexual assault, this data must accordingly be considered personal data *in connection with* that criminal case. When connected to a criminal case, the data should be excluded from the Authority’s mandate to issue orders cf. section 60(1) in order to avoid interfering with the police’s investigation. The police does, however, suggest that this is wrong.

According to the police, the term “in connection with” must be interpreted in light of the relevant registry. If the assessment relates to the police log, this data will never be data *in connection with* a criminal case due to the fact that the police log is not a criminal registry.
The police log contains both personal data and other data relating to “all important circumstances and information relating to the organization, planning and execution of the Police’s services”\textsuperscript{143}. It is practically a collection of data such as names and addresses, but also explanations and experiences coming from the Police, witnesses and other sources.

If, however, the assessment relates to data processed in a criminal case registry, the relevant data will be considered data \textit{in connection with} a criminal case. When the police establishes a criminal case, they also establish a registry for the investigation of that particular offense. The police stores everything they need for the investigation of this particular case in that registry. This is why data in the police log is never connected to a criminal case. The data processed in the police log might be interesting in the beginning of a criminal investigation, but only in order to find witnesses and other sources of information which the Police may investigate further.

As for what is indeed considered data \textit{in connection with} a criminal case, this will in essence be the data stored in the mentioned criminal files.

The Authority has in the relevant cases mentioned the importance of not interfering with the police’s investigations. The police’s current practice maintains the purposes underlying the separation of the Authority’s powers. If personal data is erased or rectified in the police log, it cannot interfere with a criminal investigation. Firstly, data in the police log cannot be used as evidence in a criminal investigation due to the fact that it is merely the police’s and civilians’ perception of the reality. If the police would need the police log for a criminal investigation, it would as mentioned be to find sources which they must follow up in order to create material they can use in the investigation.

It should further be mentioned that the requirements for erasure and rectification in the police log under the Police Databases Act are much stricter than under the GDPR\textsuperscript{144}. This means that there must be a case of wrongful registration of objective information, like names and addresses, for

\begin{itemize}
\item \textsuperscript{143} Cf. section 53-1 no. 2 of the Police Database Regulation
\item \textsuperscript{144} The data quality principle in Article 5(1) d) GDPR and in section 6 of the Police Databases Act are not the same. Section 6(2) gives the Police a possibility to process unverified personal data, which may be incorrect.
\end{itemize}
erasure and rectification to be permitted\textsuperscript{145}. If a wrong name or address has been deleted or erased from the police log, this can hardly interfere with the Police’s investigation, as it will not be usable.

To conclude, all personal data processed in the police log is considered processing of personal data “not in connection with” a criminal case cf. section 60(1) in line with the police’s current practice. Personal data processed in the individual criminal files shall be assessed according to the provisions relating to processing of personal data “other than in individual criminal cases” cf. section 60(2).

4.3.2 Section 60(3) of the Police Databases Act – may the claimant appeal a decision which establishes lawful processing?

4.3.2.1 Explaining the problem

The Directorate has further raised questions relating to the Board’s dismissals of the Authority’s decisions not to issue appeals to the police. This might threaten the data subject’s right to an appeal\textsuperscript{146}.

4.3.2.2 The Directorate’s inquiry

In the Directorate’s inquiry to the Justice Department, they state that the Board has wrongfully denied the data subject a right to appeal the Authority’s decision establishing that the police processed personal data lawfully. This critique is directed to the case PVN 2018/19, but the question is also relevant in connection with the case PVN 2018/17 as the data subject was denied appeal here as well on the same grounds.

In the case PVN 2018/19, the Board stated that “it is only the Authority’s decisions to issue orders that may be appealed to the Board, not a decision that processing of personal data is lawful pursuant to the Police Databases Act, and therefore does not give reason to issue an order.”

\textsuperscript{145} Ot.prp.nr. 108 (2008-2009) page 296

\textsuperscript{146} Cf. section 22(2) of the Personal Data Act 2018 and Article 78 GDPR
4.3.2.3 An assessment of section 60(3)

Section 60(3) in the Police Databases Act describes the requirements for an appeal to the Board: “The Data Protection Authority’s decisions pursuant to the first paragraph can be appealed to the Privacy Appeals Board.”

The Police Directorate assumes that the data subject must have a right to appeal the case also when the Authority finds that the Police has processed the relevant personal data lawfully and does not issue an order. The Board disagrees, and states that only decisions to issue orders are subject to appeal. The latter would entail that decisions going against the data subject’s interests could never be appealed.

The question of whether decisions not to issue orders are subject to appeal must be solved on the basis of an interpretation of the term “decisions pursuant to the first paragraph”. There are two key elements: (i) “decisions” and (ii) “pursuant to the first paragraph”.

As for the criterion “pursuant to the first paragraph”, this limits the appeals possibility to orders, thus excluding decisions relating to reprimands from being appealed. This is in line with the Board’s general mandate enshrined in section 22(2) of the Personal Data Act, as a decision to issue a reprimand is not an “administrative decision” 147.

The term “decision” in section 60(3) must be interpreted in accordance with “administrative decision” cf. section 2(1) a) of the Public Administration Act 148, which “generally or specifically determines the rights or duties” of private persons cf. section 2(1) a) of the Public Administration Act.

Does a decision not to afford a data subject a particular right enshrined in the Police Databases Act “generally or specifically determine the rights or duties” of the data subject?

---

147 Cf. section 22(2) of the Personal Data Act 2018 and section 2(1) a) of the Public Administration Act, also Article 78(1) GDPR requiring a “legally binding decision” which a reprimand is not.

148 The footnote connected to section 60 (3) leads to section 22 in the Personal Data Act establishing that “decisions” cf. section 2(1) a) in the Public Administration Act may be appealed to the Board.
The Board refers to the preparatory works to support their interpretation: “Because orders will regularly be directed towards the controller, also the controller will be able to appeal the Authority’s decisions.” One may disagree that the preparatory works support the Board’s position; the only logical explanation for explicitly writing that “also the controller” may appeal the Authority’s decisions, is that at least the data subject – the other involved party – will be able to appeal the decisions.

Eckhoff writes in relation to section 2(1) a) that “Determinative for the rights or duties are also decisions that determine with a legally binding effect whether or not a right exists pursuant to the applicable general provisions”. A decision denying “A” a right to erasure or rectification is thus an “administrative decision”, which subjects the decision to appeals cf. section 60(3) of the Police Databases Act. The data subject is especially in need for an appeals solution when they are not afforded rights in the individual case, making this a good norm.

During a telephone conversation with the Disciplinary Director in the Justice Department’s police department, whom had a lead role in writing the Police Databases Act, it was mentioned that it was clear that the data subject should be able to appeal decisions made by the Authority relating to orders cf. section 60(1). They did not consider it necessary to specify this in the legal text.

To conclude, decisions not to issue orders are subject to appeal cf. section 60(3) of the Police Databases Act. Considering the fact that the Board’s positions contrary to this conclusion are very recent, and that the same interpretation prevails in the Board today, this would suggest that a change of regulation in section 60(3) is necessary in order to ensure rightful appeals in the future.

149 Ot.prp.nr.108 (2008-2009) page 325
150 Eckhoff (2018) page 260
151 Cf. section 2(1) a) of the Public Administration Act
152 Cf. also section 2(1) a) of the Public Administration Act, cf. section 22(2) of the Personal Data Act
153 This position was established in the cases PVN 2018/17 and 19
154 The matter was discussed with the current Board chairman, whom confirmed that the Board claimed that their interpretations in 2018 were correct, although it might be subject to discussion.
5 Conclusion

Enforcement is indeed the backbone of the rule of law. Without a strong enforcement, the rights of data subjects might become illusory. A strong enforcement requires the enforcement agencies to establish the de lege lata on a justifiable basis. There is reason to question some of the legal positions acquired by the Authority and the Board since the Board’s establishment in 2001.

Both agencies have questioned each other’s legal positions frequently on a case-by-case basis. The agencies’ legal positions have also been challenged by the National Police Directorate and the Justice Department, having an interest in how data protection law is enforced.

This thesis has suggested that the Authority and the Board have made questionable interpretations of fundamental legal concepts such as “administrative decision” cf. section 2(1) a) of the Public Administration Act and the restrictions of processing special category data in section 9 of the Personal Data Act 2000 and section 11 of the Personal Data Act 2018 cf. Article 9 GDPR. Also, the Board has accepted an interpretation of consent relating to parents’ consent on behalf of their children that both the Authority and the writer of this thesis suggest challenge fundamental elements of a valid consent.

This thesis has further suggested that the Authority and the Board may have shown an insufficient understanding of vital factual circumstances necessary for the interpretation of the Police Databases Act. This has affected the Authority’s mandate to issue orders as well as the claimant’s right to an appeal. One must however consider the possibility that the Authority and the Police are manifestly in disagreement in the intersection of general data protection law and the police’s processing of personal data regulated in the Police Databases Act. The disagreements relating to the subject’s right to an appeal has led to a suggestion for a change of regulation in section 60(3) of the Police Databases Act.

On a more general level, this thesis has aimed to summarize the most relevant available sources for interpretation of the mentioned areas of data protection law. These collectively suggest that the Authority and the Board may reconsider their legal positions in the relevant data protection matters.
## 6 Table of reference

### Sources of law

<table>
<thead>
<tr>
<th>Year</th>
<th>Act/Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>Act 15(^{th}) of June 2018 no. 38 relating to the processing of personal data (the Personal Data Act 2018)</td>
</tr>
<tr>
<td>2018</td>
<td>Regulation 15(^{th}) of June 2018 no. 876 relating to the processing of personal data (the Personal Data Regulation)</td>
</tr>
<tr>
<td>2014</td>
<td>Act 20(^{th}) June 2014 no. 43 relating to personal health filing systems and the processing of personal health data (Personal Health Data Filing System Act)</td>
</tr>
<tr>
<td>2013</td>
<td>Regulation 20(^{th}) of September 2013 no. 1097 relating to the processing of data by the police and the prosecuting authority (the Police Databases Regulation)</td>
</tr>
<tr>
<td>2010</td>
<td>Act 28(^{th}) of May 2010 no. 16 relating to the processing of data by the police and the prosecuting authority (the Police Databases Act)</td>
</tr>
<tr>
<td>2005</td>
<td>Act 17(^{th}) of June 2005 no. 90 relating to mediation and procedure in civil disputes (the Civil Procedure Act)</td>
</tr>
<tr>
<td>2001</td>
<td>Act 18(^{th}) May 2001 no. 24 relating to personal health filing systems and the processing of personal health data (Personal Health Data Filing System Act)</td>
</tr>
<tr>
<td>2000</td>
<td>Act 14(^{th}) of April 2000 no. 31 relating to the processing of personal data (the Personal Data Act 2000)</td>
</tr>
<tr>
<td>Year</td>
<td>Act</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>2000</td>
<td>Regulation 15&lt;sup&gt;th&lt;/sup&gt; of December 2000 no. 1265 relating to the</td>
</tr>
<tr>
<td>1999</td>
<td>Act 16&lt;sup&gt;th&lt;/sup&gt; July 1999 no. 66 relating to the Schengen</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1978</td>
<td>Act 9&lt;sup&gt;th&lt;/sup&gt; of June 1978 relating to personal data filing</td>
</tr>
<tr>
<td></td>
<td>systems (the Personal Data Filing System Act)</td>
</tr>
<tr>
<td>1967</td>
<td>Act 10&lt;sup&gt;th&lt;/sup&gt; of February 1967 relating to procedure in cases</td>
</tr>
<tr>
<td></td>
<td>relating to procedure in cases concerning the public administration</td>
</tr>
<tr>
<td></td>
<td>(the Public Administration Act)</td>
</tr>
<tr>
<td></td>
<td>Prop. 72 L (2013-2014)</td>
</tr>
<tr>
<td></td>
<td>Prop. 47 L (2011-2012)</td>
</tr>
<tr>
<td></td>
<td>Ot.prp. nr. 108 (2008-2009)</td>
</tr>
<tr>
<td></td>
<td>Ot.prp. nr. 5 (1999-2000)</td>
</tr>
<tr>
<td></td>
<td>Ot.prp. nr. 92 (1998-1999)</td>
</tr>
<tr>
<td></td>
<td>NOU 1997: 19</td>
</tr>
</tbody>
</table>
Reg 2016/679/EU  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)

Dir 95/46/EC/EU  Directive 95/46/EC of the European Parliament and of the Council on 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive)

ECHR  Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 4th of November 1950

Literature


**Other sources**

• Ministry of Local Government and Modernisation “Instruks for Personvernnemnda”, adopted 23rd of October 2018

• Article 29 Data Protection Working Party “Opinion 15/2011 on the definition of consent”, adopted on 13th of July 2011


• European Data Protection Board “Guidelines 3/2019 on the processing of personal data through video devices”, adopted on 10th of July 2019

• All 270 cases from the Privacy Appeals Board have been read and used during the research for this thesis. They are available at: https://www.personvernnemnda.no/avgjorelser

**Case law:**

• Case C-136/17 Google v CNIL  
  ECLI:EU:C:2019:773

• Case C-222/84 Johnston v Chief Constable of the Royal Ulster Constabulary  
  ECLI:EU:C:1986:206
• Case C-222/86 Heylens and others v Unectef
  ECLI:EU:C:1987:442

• Case E-15/10 Posten Norge v EFTA Surveillance Authority

*Yearly reports from the Authority and the Board:*


• The Norwegian Data Protection Authority “Årsrapport for 2018 – Tall og tendenser fra Datatilsynets virksomhet”. Retrieved 31.10.2019. Available at:

• The Norwegian Data Protection Authority «Årsmelding for 2017 – Hva preget året som gikk på personvernfeltet, og hvilke utfordringer ser Datatilsynet fremover?» Retrieved 31.10.2019. Available at:

• The Norwegian Data Protection Authority «Årsmelding for 2016 – Hva skjer på personvernfeltet, og hvilke utfordringer ser vi fremover?» Retrieved 31.10.219. Available at:

• The Norwegian Data Protection Authority «Årsmelding for 2015 – Hva rører seg på personvernfeltet?» Retrieved 31.10.2019. Available at:


Accessed documents through access request:

Relating to the case PVN 2015/06:

• Letter from the Data Protection Authority to the Privacy Appeals Board dated 22.01.2015 “Oversendelse til Personvernnemnda – Klage på avslag om sletting av søketreff I Google”

Relating to the case PVN 2016/10:

• Letter from the Data Protection Authority to the Privacy Appeals Board dated 24.06.2016 “Oversendelse av klagesak til Personvernnemnda – Klage over pålegg om å slette søketreff I søkemotoren Google”

• Letter from the Data Protection Authority to the Privacy Appeals Board dated 20.10.2017 “Oversendelse av klagesak til Personvernnemnda – klage over avslag om å slette søketreff I søkemotoren Google”

• Letter from the Data Protection Authority to the Privacy Appeals Board dated 22.03.2018 “Oversendelse til Personvernnemnda – Sletting av søketreff I søkemotoren Google”
Relating to the case PVN 2018/03:

- Letter from the Data Protection Authority to the Privacy Appeals Board dated 26.02.2018 “Oversendelse til Personvernnemnda – Klage på delvis avslag på søknad om forlengelse og utvidelse av konsesjon til å behandle personopplysninger – Nasjonalt tvillingregister”

Relating to the cases PVN 2018/17 and PVN 2018/19:

- Letter (regarding an access request and erasure) from the appellant to the National Criminal Investigation Service dated 07.05.2016

- Letter from the National Criminal Investigation Service dated 12.10.2016 “Vedrørende begjæring om innsyn og sletting av opplysninger”

- Letter from the appellant (response to the Service’s decision) to the National Criminal Investigation Service dated 19.10.2016

- Letter from the National Police Directorate to the appellant dated 01.02.2017 «Vedtak – Klage over avslag på begjæring om sletting og retting av opplysninger»

- Letter from the appellant (appeal on the Directorate’s decision) to the Data Protection Authority dated 08.03.2017 «Sak om sletting av opplysninger i politioperativt register»

- Letter from the Data Protection Authority to the National Criminal Investigation Service dated 13.07.2017 “Krav om redegjørelse vedrørende avslag på begjæring om retting og sletting i politioperativt register”

- Letter from the National Criminal Investigation Service to the Data Protection Authority dated 01.09.2017 «Redegjørelse vedrørende avslag på begjæring om retting og sletting i politioperativt register»
• Letter from the Data Protection Authority to the appellant dated 21.12.2017 «Sak vedrørende sletting og retting av opplysninger i Politioperativt register – avslutning av sak»

• Letter from the Data Protection Authority to the Privacy Appeals Board dated 29.06.2018 «Oversendelse til Personvernnemnda – Klage på avgjørelse om avslutning av sak»

• E-mail from the National Police Directorate to the Justice Department dated 12. August 2019 15:58

• Letter from the Authority to the Board dated 10.07.2018 “Oversendelse til Personvernnemnda – Klage på Datatilsnets beslutning om avslutning av sak – Krav om sletting av opplysninger I politiets registre”

• Letter from the Authority to the Board dated 30.01.2019 «Datatilsynets bemerkning til lovvalget»

• Letter from the Authority to the Board dated 26.06.2018 «Oversendelse til Personvernnemnda – Klage på avgjørelse om avslutning av sak»

• Letter from the Authority to the Board dated 30.01.2019 «Datatilsynets bemerkning til lovvalget»