UiO : Faculty of Law
University of Oslo

Use of fingerprints in private sector - Norwegian data privacy perspective

Candidate number: 8013

Submission deadline: 01/12/15

Number of words: 17,866

Table of contents

Contents

1 INTRODUCTION 1

1.1 Background 1

1.2 Objective 2

1.3 Methodology and structure 3

1.4 Definitions 4

2 II BIOMETRICS (AND FINGERPRINTS IN PARTICULAR) IN PRIVATE SECTOR 5

2.1 What is biometrics? 5

2.1.1 How does it work? 6

2.1.2 What does it do? 8

2.2 Fingerprint biometrics 10

2.2.1 Current technological development in the private sector 10

3 III CURRENT NORWEGIAN RULES 16

3.1 Legal framework 16

3.1.1 Article 12 of the Personal Data Act 17

3.1.2 General rules for processing personal data 18

3.2 Case law 23

4 IV TECHNOLOGICAL DEVELOPMENT AND NORWEGIAN RULES 36

4.1 Fingerprint regeneration 36

4.1.1 Is it possible to regenerate an image from the template? 36
4.1.2 How does it affect current interpretation of the Norwegian rules? 38
4.1.3 Conclusion 41

4.2 The Cloud 42
4.2.1 Biometrics as a service 43
4.2.2 How does it affect current interpretation of the Norwegian rules? 47
4.2.3 Conclusion 48

4.3 Mobile outburst (and e-payment) 49
4.3.1 How does it work? 49
4.3.2 How does it affect data privacy? 52
4.3.3 Conclusion 53

5 CONCLUSION 54

6 TABLE OF REFERENCE 56

1 INTRODUCTION

1.1 Background

Use of biometrics, in plain terms means measuring one or more physical (as well as behavioral) characteristics of a human body, in order to determine or verify one's identity[1]. The most dominant form of biometric application is, without doubt, the use of fingerprints, which gained popularity by its application by public authorities (police and customs authorities) and which developed as early as in the 1920s. Nowadays, a significant shift has been made, as fingerprint biometrics is used more and more in the private sector, primarily due to technological developments which made equipment and knowledge easily accessible to private actors (both companies and individuals). But this turn of events has its consequences on the protection of the right to privacy and the right to protection of personal data[2]. Application of fingerprint biometrics in private sector will, in many cases, trigger the application of data protection laws, and this paper will examine its use from the Norwegian perspective.

The Norwegian Personal Data Act from 2000 sets out a legal regime for processing personal data, including the use of biometrics, which is governed by its article 12. An important role in the interpretation and application of the law is played by the Norwegian Data Inspectorate (first instance) and The Privacy Appeals Board (second instance) whose decisions influence heavily the use and application of fingerprint biometrics in Norway. Even though the law technically, was not amended on the point, last interpretation of the rules occurred in 2012.

However, the technological progress naturally continued since then, and it is the purpose of this paper to examine the adequacy of the Norwegian data protection law as it is currently

---

[1] *See* Article 29 Data Protection Working Party's Opinion 3/2012 on developments in biometric technologies, pg. 1-5

[2] *See* Privacy and Data Protection Issues of Biometric Applications, Els J. Kindt, Springer Science+Business Media Dordrecht 2013, at pg 18

interpreted, with the evolution of both biometric technology itself, and the new fields of its application (such as private sector application in the cloud and mobile devices).

1.2 Objective

The objective of this paper is to scrutinize the current status of Norwegian data protection law on use of fingerprints in private sector, and to assess its adequacy, in terms of technological progress and development that occurred since the last interpretation of the Personal Data Act on this point. Thus, this paper will discuss both the way in which the Norwegians regulated this area, and the way they interpret the law, but the stronger emphasis shall be placed on the way the law is currently interpreted.

The hypothesis of the thesis is: "Interpretation of the Norwegian data protection rules on the use of fingerprints in private sector is inadequate in the light of current state of technology". In order to test the hypothesis, the main research question that needs to be answered is: are the Norwegian data privacy rules, governing the use of fingerprints in the private sector, too strict, or do they fail to protect data subject's privacy? The question shall be answered in the light of technological and technical progress, which is made since the last interpretation of data privacy rules in 2012, by the Privacy Appeals Board (shall be referred to interchangeably as: the Board). In order to answer this question, additional sub questions must be raised. First sub question is:

- what are current data protection rules on the use of fingerprints in private sector in Norway?

Second sub question is twofold and it contains two related questions:

- what is the current state of the art in the area of fingerprint biometrics, and
- do current data protection rules cover the current state of the art?

Final sub question is:

- how does current state of the art affect current interpretation of the rules?

The focus of the thesis will be on private sector use only (which shall be defined in the coming sections) due to the fact that processing of personal data by public agencies and authorities is, in part, falling outside the scope of general data protection rules e.g. finger-

print processing in criminal matters, border control etc[3]. This paper will only focus on general legal framework on data protection that as opposed to the legal framework governing fingerprint processing activities by state actors.

1.3 Methodology and structure

Firstly, I will begin with a technical description of a biometric system (fingerprint biometrics in particular). Here, a descriptive research method shall be used to explain how a biometric system works, and how it triggers the application of the data protection laws. This part shall have the focus on the way in which biometric systems work in general, as well as the current state of the art in the field of fingerprint biometrics.

Secondly, I will perform the doctrinal analysis, which shall consist of interpretation and systematization of current legal norms governing the use of fingerprints in private sector. The central focus of this part shall be on the Norwegian implementing legislation (Personal Data Act and) of the Directive 95/46/EC. Qualitative analysis of the Directive itself shall also be undertaken, but mainly in the function of understanding the Norwegian law on the point. Doctrinal analysis approach shall further be used to the case law of The Privacy Appeals Board, in order to 'ascertain the precise state of the law on a point'.

Third and final part of the research will build upon first two parts, through a method of case studies. A number of instances of the same phenomenon (advancement in the biometric technology) shall firstly be identified[4]. They will then be studied through the prism of current Norwegian data protection regime. The research objective will be the analysis of adequacy of current rules to the technological advancement. This research objective will guide the selection and analysis of cases within the class or subclass of the phenomenon under investigation[5].

---

[3] *See* § 3. 4e ledd Lov om behandling av personopplysninger (personopplysningsloven) and Article 3 (2) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] Case Studies and Theory Development in the Social Sciences, George & Bennett, Belfer Center Studies in International Security 2005, Chapter 3 pg. 67-71

[5] Ibid.

1.4 Definitions

The following definitions are set out in order to fully understand the scope of this paper, and to set boundaries to the issues this paper shall, and shall not address.

Use of fingerprints – use of friction ridges' pattern, found on individual's finger, for biometric recognition. Biometric recognition, for the purpose of this paper should be understood as both identification (comparing biometric data of an individual acquired at the time of the identification to a number of biometric templates stored in a database[6]) and verification (comparing the biometric data of an individual acquired at the time of the verification to a single biometric template stored in a device[7]).

Private sector – the processing operations that fall outside the scope of operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

For the purpose of this paper, it is defined negatively as the operations falling out of the public sector operations, enumerated above. Examples of private sector use would be: workforce management (biometric time and attendance systems), use of biometrics in banking systems and financial institutions, mobile biometrics (use of biometrics on mobile devices such as smartphones and tablets), private actors' access control (access to areas, shops, facilities in non-governmental context).

Norwegian perspective – the primary focus of the paper shall be on the Norwegian legislation and practice of the Norwegian data protection authorities. Full attention shall be given to the way the law is being interpreted, and the paper will not discuss eventual flaws of the legislative solutions, nor shall it propose changes to the legislation itself. The focus will rather be on the current interpretation of the existing rules.

---

[6] Supra note 1. pg. 5-6

[7] Ibid.

2 II BIOMETRICS (AND FINGERPRINTS IN PARTICULAR) IN PRIVATE SECTOR

2.1 What is biometrics?

Ever since the beginning of humanity, people have used biological or behavioral traits to recognize each other, e.g. facial recognition (I recognize John because I know how his face looks like) or gait recognition (I recognize John from distance even though I can't see his face, because I know the way he walks, which is unique to him). Given the current world population of almost 7,5 billion people[8], identifying individuals and associating rights and obligations to them has become more important than ever. This is why the use of biometrics has grown in both its application and importance.

In order to understand the notion of biometrics, one needs firstly to understand the term 'biometric data'. Article 29 Working Party defines it as: "biological properties, behavioral aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable...[9]." Biometrics could therefore be defined as a science or a method of analyzing biometric data in order to identify an individual or verify its identity[10]. Additional way of defining biometrics would be as "a physiological or behavioral trait which may be measured, recorded and subsequently compared to another sample in order to confirm an individual's claimed identity.[11]" All this takes place with the help of a biometric system, which is simply put, a group of devices and processes used for the application of biometrics measurement.

---

[8] http://www.census.gov/popclock/ US Census Bureau's U.S. and World Population Clock, last visited on 30/09/15 at 12:09

[9] Supra note 1. pg 3.

[10] *See* Introduction to biometrics, Anil K. Jain, Arun A. Ross and Karthik Nandakumar, Springer Science+Business Media, LLC 2011, at pg 2.

[11] Practical Biometrics - From Aspiration to Implementation, Julian Ashbourn, Springer-Verlag London 2004, 2015, pg 1.

2.1.1 How does it work?

Modern biometric system operates in two stages: **enrollment stage** and **recognition stage**. Enrollment stage precedes the recognition stage, and consists of acquiring the (biometric) data from an individual and depositing collected information usually in a database of some kind. Collected information is not stored by itself, but it is linked to the individual's person's identity. Afterwards, the recognition stage can be deployed, when the system operator re-acquires biometric data, and compares it to saved data (from enrollment stage) in order to get a match (and identify an individual or verify its identity)[12].

2.1.1.1 Enrollment stage

In order to begin the enrollment stage, one needs to set up a user interface and a suitable sensor to capture biometric data of an individual. The sensor must capture 'raw[13]' biometric data of satisfactory quality, and further process it through the feature extraction stage. Before feature extraction, it is possible that the system performs quality assessment (to determine if the image is suitable for further processing), segmentation (if the raw data is of satisfactory quality, then the system usually isolates required data from the background noise), and enhancement (segmented biometric data is subjected to a signal quality enhancement algorithm in order to improve its quality and further reduce the noise) of the raw image[14].

In the feature extraction stage, raw biometric data is converted into a 'template'. This means that only the necessary information (to single out an individual from the others) is collected from the raw image, and saved in the system for further use (in the recognition stage) either as a minutia map or more commonly as a data stream, as seen on the Image

[12] Supra note 2. pg 4.

[13] 'Raw' biometric data could is an unaltered biometric data captured by the sensor 'as is' e.g. an image of the fingerprint.

[14] Supra note 2. pg 6.

1[15]. Upon obtaining a template, it needs to be stored for further reference, and this can be done at a database or a card or other suitable remote object held by the individual.

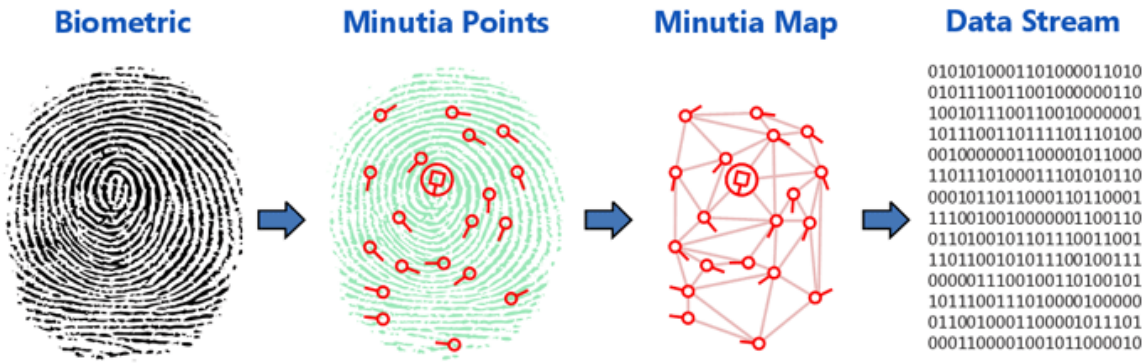

Image 1. From left to right shows: 1) raw data, 2) necessary information to single out and individual from others without the use of raw image (minutia points), 3) only minutia points without the rest of the raw data image (minutia map), and 4) algorithm of minutia map which is only machine readable (data stream).

2.1.1.2 Recognition stage

At this stage, the individual is once again exposed to the sensor, where new biometric data is collected and processed, as it is done in the enrollment stage. The sample that is made that way is then compared to the already collected 'template'. This system is best illustrated by the **Image 2.** (created by the author).

[15] Image obtained at http://www.identityone.net/BiometricTechnology.aspx last visited 30/09/15 at 13:04

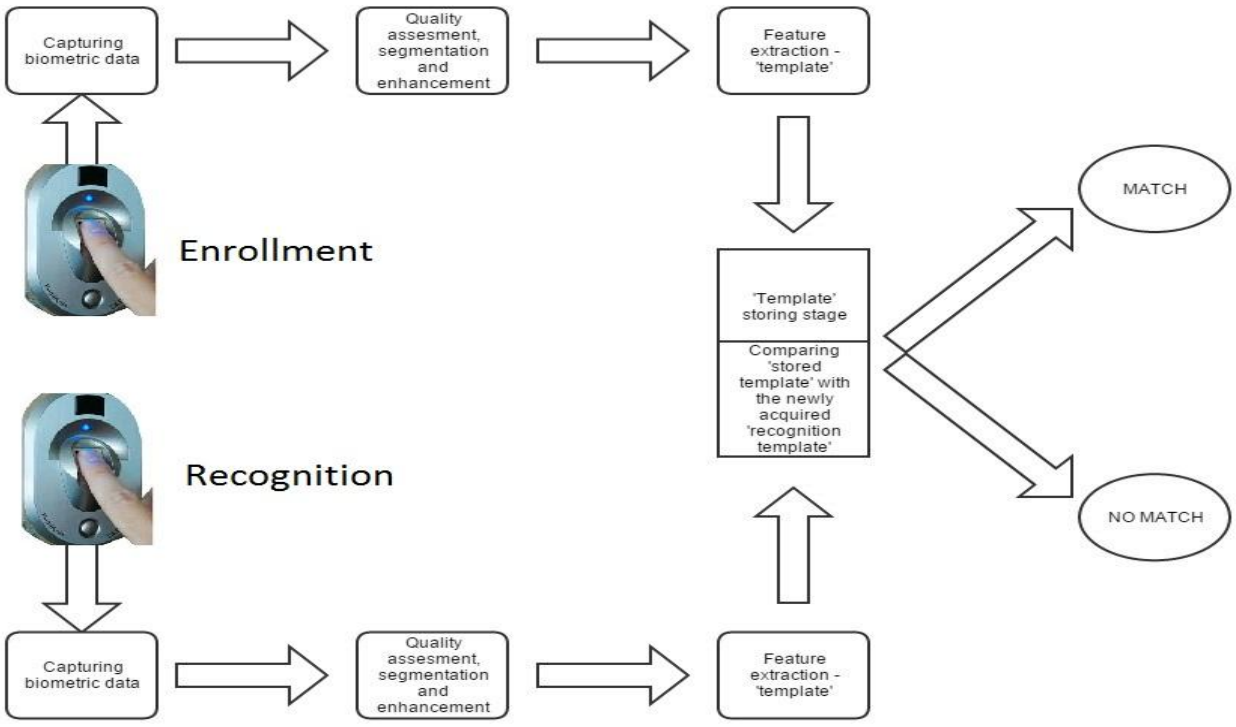

Image 2. Biometric system operation scheme

2.1.2 What does it do?

The most common purpose of the biometric system is to provide two basic identity management functionalities: verification and identification[16]. **Verification** occurs when the data subject claims an identity and the system verifies whether the claim is accurate or not. The basic question answered by the biometric system in this stage is: "Am I who I claim I am?" and the query ('template' obtained in at the recognition stage) is compared only to one template - the one of the claim identity. Due to its one-to-one nature, verification is usually made with the use of a token or PIN[17]. **Identification** is usually divided in two functionality groups: positive and negative. Positive identification answers the question of whether the

[16] Supra note 11. at pg 10-11.

[17] Ibid

data subject is known to the system. This is done by comparing the recognition or query 'template' with the set of already stored 'templates' from the enrollment stage, usually from the database. In this context, normally all templates stored in the database are being proofed against the 'query template'. Negative identification, also known as 'screening', answers the question: "Am I who I say I am not?. The purpose of negative identification is to prevent a single person from using multiple identities or obtaining multiple benefits she is not entitled to[18].

Application of biometric systems is not error free, and it is in fact hard to produce 100% pure match between 'original[19]' and 'query template'. That is why we have the False Accept Rate and the False Reject Rate. **False Accept Rate** is the probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. It measures the percentage of invalid inputs which are incorrectly accepted. **False Reject Rate** is the probability that the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template[20].

Not all biometrics are ideal for application of biometric systems, but some of them are certainly more likely to give positive results than others. Fingerprints are certainly among those who are used the most, and it is done so because they are more or less[21]: unique (different for every individual), universal (every individual has them), measurable and permanent (to a certain degree they remain unchanged)[22]. The following subchapter will introduce the fingerprint biometrics before moving to legal analysis.

---

[18] Ibid.

[19] Template obtained at the enrollment stage.

[20] Supra note 1. at pg. 6.

[21] Some exceptions exist, but they are not that often.

[22] Supra note 11. at pg. 29-30.

2.2 Fingerprint biometrics

Use of fingerprints in biometrics has become a commonplace today. Not only because fingerprints have the qualities (unique, universal, measurable and permanent) required for their use in a biometric system, but also because the product market for equipment and software has matured. Sensors have become cheaper, more compact and for the most of them, the accuracy went to 99%. Additionally, such technology has gone mobile, so the mobile ID terminals are a common thing today. Finally, the US Federal Bureau of Investigation (FBI) has developed the Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) standard as a reference. The FIPS 201 PIV standard has become the accepted metric worldwide for fingerprint sensor quality[23]. But what exactly are fingerprints, and how does fingerprint biometrics work?

Fingerprint can be defined as the reproduction of the exterior appearance of the fingertip epidermis, i.e. the pattern of interleaved ridges and valleys on the tip of a finger[24]. The pattern of friction ridges on the tip of the finger is fully formed even before birth (at about 7 months of fetus development) and they should remain unchanged throughout the life of an individual (unless external factors such as accidents or sickness affect them), and that is why they are suitable for application in biometric systems[25].

2.2.1 Current technological development in the private sector

It has been almost 4 years since the last decision of the Privacy Appeals Board in the area of fingerprint processing and data privacy. Both the technology and the areas of application have changed since, and now I will shortly examine the novelties in this area.

---

[23] Fingerprint biometrics in the real world, Chris Trytten, Biometric Technology Today, June 2012.

[24] Supra note 11. at pg. 51.

[25] Handbook of Fingerprint Recognition, D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Springer-Verlag London Limited 2009 at pg 34.

2.2.1.1 Mobile outburst

Even though the use of fingerprints on mobile devices is not exactly a new thing[26], the novelty is the increase in use of fingerprint biometrics on the smartphones. In 2013 Apple added fingerprint scanner to its iPhone 5s model, which was followed by the HTC with its One Max model as well as Samsung Galaxy S5[27]. Both iPhone 5s and Galaxy S5 were most sold models in 2014 at both Elkjøp, Expert, Euronics and Komplett.no, which are the leading retailers in the electronics market in Norway. These phones top first two places in all of these four retailers, and it is important to stress out that these are last year's models[28]. Exact numbers are not available, but the Consumer Electronics Trade Foundation in its report stated that the Norwegians bought 1.953.000 smartphones in 2014 and approximately same number is expected to be purchased in 2015[29]. Also newer models (2015), such as iPhone 6s and 6s+, Galaxy S6, Galaxy S6 Edge, HTC One Max and One Plus have integrated fingerprint sensors[30] so we could assume that by the end of 2015, we will have at least ¼ of Norwegian population with fingerprint processing devices (biometric systems) in their pockets and purses[31].

2.2.1.2 The Cloud

Biometric system is, in most instances, a part of a more general system. It is hard to imagine a fingerprint authentication system which exists only to scan fingerprints. There is al-

---

[26] One of the first cases of the Privacy Appeals Board has dealt with the use of fingerprints on the Lenovo laptops in 2006 - PVN-2006-7.

[27] http://webcusp.com/list-of-all-fingerprint-scanner-enabled-smartphones/ last visited on 05/10/15 at 11:06

[28] http://www.dagbladet.no/2015/02/17/tema/dinside/aller/mobil/teknologi/37758810/ last visited on 05/10/15 at 11:10

[29] http://www.elektronikkbransjen.no/Presse/Omsetningstall-og-presentasjoner last visited on 05/10/15 at 11:15

[30] Supra note 28.

[31] Through Telenor sales channels, in April 2015, top 5 sold smartphones were smartphones having integrated fingerprint sensor.

ways some further purpose of the biometric system, that being either authorization or identification, in order to accomplish some specified purpose (e.g. labor force management, or management of access to certain facilities). Usually, these biometric systems were relying on the infrastructure that exists on the spot, i.e. businesses acquired and stored in-house all the equipment. But given the costs of this enterprise, it has become more and more frequent to use 'cloud services' in order to house the necessary infrastructure at the 'cloud services' provider.

National Institute of Standards and Technology defines 'cloud computing' as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Using a biometric system in the Cloud means that the business does not have to house the infrastructure anymore, but the infrastructure is housed at the 'cloud services provider', which makes it available to the business. Provider houses the servers containing 'template databases', network connectivity, and all the processing actions necessary in both enrollment and recognition stages, for both verification and identification. Business using 'cloud services' only needs to have a fingerprint scanner set up, and everything else is left for the provider to do[32].

This development changes drastically the scenario for the use of biometric systems, given the fact that the costs have been minimized, and the systems can be used even by the small enterprises. But it also has effect on the data being processed, since it changes the way in which the biometric system operates. Business employing biometric systems would lose control over the process. 'Templates' will likely end up in the hands of the 'cloud services provider'. That can be the case of the raw images as well (as no control exercised by the controller in the fingerprint collection and processing stages). The rise of the 'cloud computing' must be regarded when protecting data privacy in the modern age.

[32] Biometrics in the cloud What does cloud computing mean for biometric systems? Davi Ras, Keesing Journal of Documents & Identity, February 2013

2.2.1.3 Fingerprint regeneration

The core of cohabitation between all biometric systems and data privacy law is the use of biometric 'templates' instead of raw images. This presupposes that the templates are more pro-privacy than raw images. Article 29 Working Party prescribes that a 'template' should be extracted in a way that is specific to that biometric system, and not used by other controllers of similar systems in order to make sure that a person can only be identified in those biometric systems that have a legal basis for this operation[33].

For a long time, it has been assumed that fingerprint images could not be reconstructed from 'templates'. Many researchers and practitioners in the field claimed that the 'template' does not include enough information to reconstruct the original fingerprint image[34]. Even some 10 years ago, it was possible to reverse-engineer biometric templates to fingerprint images to some degree[35]. After thorough research and experiments, the result was drawn that is definitely possible to successfully attack state-of-the-art automatic recognition systems, provided that one is able to present reconstructed images to the system, with the average percentage of successful attacks against nine different systems was 81 percent at a high security level, and 90 percent at a medium security level[36].Since then, other algorithms were also developed which helped to reconstruct the entire algorithms from the minutiae template[37].

---

[33] Supra note 1. at pg. 31.

[34] Fingerprint Image Reconstruction from Standard Templates, R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, SEPTEMBER 2007 at pg. 1489.

[35] Legal effects of this shall be discussed later in thesis.

[36] Supra note 35. at pg. 1502.

[37] *See* Fingerprint Reconstruction: From Minutiae, B. Amminaidu and V. Sreerama Murithy, Advances in Intelligent Systems and Computing vol 249, Springer International Publishing Switzerland 2014, , at pg. 79-86.

2.2.1.4 E-payment

One thing that certainly affects abovementioned points is the rise of e-payment services that use fingerprint recognition methods for verification of transactions. Mastercard recently announced the roll-out of 'MasterCard Identity Check', that will enable consumers to make online payments with the use of fingerprint recognition, instead of use of PIN or other means of verification. It is expected that this method will reach Norway (among other EEA countries) in 2017[38]. But this is not the only novelty, since it is Norwegian brainpower that stands behind 'Zwipe', which is imagined to replace PIN code with the help of the fingerprint biometric system[39]. Another novelty is announced by French TSI, which plans on developing e-wallet with integrated biometric connected device (smartphone or tablet which shall be used as a fingerprint scanner)[40]. Additionally, we have Samsung Pay, Apple Pay and Android Pay, as the most popular options for payment with your smarthone, that are already alive in US, and waiting for the green light to come to Europe[41].

Given the fact that even in 2011, only 6% of all payments in Norway were made in cash[42], and the calls for cash-free Norway by 2020[43], it is easy to understand how this turn of developments may affect the data privacy regime currently in place.

---

[38] http://www.biometricupdate.com/201510/mastercard-rolling-out-payment-system-using-facial-and-fingerprint-recognition last visited on 07/10/15 at 11:58

[39] http://www.innovasjonnorge.no/no/grunder/Grunderhistorier/finger-pa-framtiden1/#.VhTtMfntmko last visited on 07/10/15 at 12:02

[40] http://www.biometricupdate.com/201509/tsi-and-trust-designer-develop-e-wallet-with-integrated-biometric-connected-device last visited on 07/10/15 at 12:09

[41] http://www.biometricupdate.com/201509/payment-service-samsung-pay-goes-live-in-the-u-s last visited on 07/10/15 at 12:16

[42] http://www.dinside.no/896430/nordmenn-foretrekker-bankkort last visited on 07/10/15 at 12:15

[43] http://www.nrk.no/norge/onsker-et-kontantfritt-norge-i-2020-1.11830344 last visited on 07/10/15 at 12:20

2.2.1.5 Conclusion

It is evident that more and more Norwegians will be using fingerprint biometric systems of some kind in the near future. With the help of smartphones, one can imagine that more and more PINs and tokens shall be replaced by biometric systems (which may also use cloud computing)[44]. This might affect interpretation of data privacy rules, as much as will data privacy rules affect the use of fingerprints in Norwegian private sector. The following chapters will turn to legal analysis of current Norwegian rules, as well as analysis of the rules in the context of the recent developments in the fingerprint biometrics field.

[44] And as soon as we have money involved, there will be high incentive to abuse the system (fraud) by tampering with the fingerprints.

3 III CURRENT NORWEGIAN RULES

3.1 Legal framework

Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act) is the central legal instrument governing data protection rules in Norway. This instrument is implementing the Directive 95/46/EC[45] (Data Protection Directive), and the Norwegian way of governing use of biometrics had an interesting genesis stemming from the Directive.

Protection of personal data in the field of biometrics in Norway is governed primarily by article 12 of the Personal Data Act. Quite surprisingly, Article 12 is primarily aimed at protecting the use of personal identification numbers, which is clear from its very heading: "Use of national identity numbers, etc.".

Article 12 reads as follows:

> *National identity numbers and other clear means of identification may only be used in the processing when there is an objective need for certain identification and the method is necessary to achieve such identification.*
>
> *The Data Inspectorate may require a controller to use such means of identification as are mentioned in the first paragraph to ensure that the personal data are of adequate quality…*

This article is implementing article 8(7) of the Data Protection Directive, which states that: "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed."

It is clear from this, that this provision is primarily aimed at protecting individuals privacy by regulating use of identification numbers, but in Norway this was extended also to biometric data, and it all happened with the inclusion of the term 'fingerprints and other biometric data' in the preparatory work of article 12. This term was included as an illustration of the term 'other clear means of identification', and no reason was given as to why the

[45] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

fingerprints (and other biometric data) were regulated in this manner. This is a bit surprising, also given the fact that this solution was unique in the Nordic countries[46] (Sweden, Denmark nor Finland), and if the legislator decided to regulate biometric data differently, at least some additional explanation was expected.

However, no additional explanation was given, and biometric data in Norway is regulated by article 12, so it was up to the Data Inspectorate and the Privacy Appeals Board, to carve up the application of the provision, and adapt it to today's standards. But before examining how it was done, analysis of the central provisions of the law affecting the work of these two bodies will be undertaken.

3.1.1 Article 12 of the Personal Data Act

Article 12, already cited above, governs the use of:

- National identity numbers and
- other clear means of identification

Preparatory work to the Personal data Act [47], already made it clear that the term 'other clear means of identification' relates to the use of fingerprints and other biometric data. The general idea behind this provision is to protect both of these from 'unnecessary use'[48]. And it does so by setting out two main conditions that could render the use of these legal. First condition is that there exists an **objective need for certain identification**. Second condition is that of necessity, and it requires that **the method used is necessary to achieve such identification**.

Both of these conditions are nicely explained through the work of the Privacy Appeals Board, and its case law will be elaborated in this paper as well. But before I start with that analysis, it must be mentioned that article 12 is not the only tool governing the processing

---

[46] *See* Notat fra Datatilsynet – forslag til revisjon av personopplysningslovens § 12 og ny bestemmelse om bruk av biometriske data at pg. 11-12

[47] Ot.prp.nr.92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven) Merknader til de enkelte paragrafene, Kappitel II, Til § 12.

[48] Ibid.

of biometric data in Norway. Even though it plays central part in the protection of biometric data, other conditions for processing, laid out by the Personal Data Act, must be abided as well.

3.1.2 General rules for processing personal data

In order for any personal data (including fingerprints and other biometric data) to be processed legally, certain conditions must be fulfilled. This relates primarily to the conditions set out in articles 8 (eventually 9) and 11. Another important part of the process is to understand the central terms and the definitions, as provided in the Act[49].

3.1.2.1 Central definitions

Article 2 of the Personal Data Act covers the basic definitions for the purpose of the Act.

Personal data is defined as any information and assessments that may be linked to a natural person. Here it is necessary to stress out that both direct and indirect identification are applicable, for the information to be personal data[50]. According to the comments to the law proposal, even the anonymized data can be personal data, if there are references or other linking points that make identification possible[51]. This is interesting, especially in the area of defining 'templates' as a personal data, which shall be discussed in later chapters. Preparatory work to the Personal Data Act is following this approach, stating that the encrypted data can also be personal data, if someone can make this data readable, and therefore identify the persons to whom the data relates to. On the other hand, preparatory work mentions specifically fingerprints as the examples of personal data[52].

Processing of personal data is defined as any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses. Preparatory work

[49] The Act is inapplicable is there is no personal data, or if it is not processed.

[50] NOU 1997:19 Et bedre personvern - forslag til lov om behandling av personopplysninger, Del III: UTVALGETS LOVFORSLAG MED MERKNADER, KAPITTEL 21. Merknader til de enkelte bestemmelsene,

[51] Ibid.

[52] Ot.prp.nr.92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven) Merknader til de enkelte paragrafene, Kappitel II, Til § 2.

to the Personal Data Act also illustrates other examples such as data transfer, search among data, blocking or deletion of data[53]. It is clear from both definition and preparatory work that these are just examples of what constitutes data processing, and the list is not exclusive. What characterizes processing is that it is purpose defined - it is performed to achieve a particular result[54].

Controller is defined as the person who determines the purpose of the processing of personal data and which means are to be used. The preparatory work is clarifying that controller can be one person or more persons jointly that assume the role of the controller[55].

Processor is defined as the person who processes personal data on behalf of the controller. This happens often, as the controller outsources data processing operations to third persons. Even though the third person processes the data, it is still the controller who assumes primarily responsibility for processing, as the Personal Data Act sets out numerous obligations to the controller, while the processor is mainly responsible to the controller. This is especially emphasized in Article 11 of the Act.

Data subject is defined as the person to whom personal data may be linked. This definition is quite clear, and it builds on the other definitions in Article 2. The preparatory work is also obscure when it comes to data subject definition, for reasons explained above.

3.1.2.2 Conditions for the processing of personal data (and sensitive personal data)

These conditions are set out in articles 8 and 9 of the Personal Data Act. In order for (any kind of) personal data to be processed legally, there has to be consent of the data subject. In the absence of the consent, processing is legal if there is statutory authority for processing, or if the processing is necessary in order to accomplish specifically stated purposes[56].

---

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] i.e. to fulfill a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract, or to enable the controller to fulfill a legal obligation, or to protect the vital interests of the data subject, or to perform a task in the public interest, or to exercise official au-

So, according to the Norwegian law, there are three different legal grounds for processing personal data. However, if the data that is being processed relates information relating to racial or ethnic origin, or political opinions, philosophical or religious beliefs, the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act, health, sex life or trade-union membership, apart from legal grounds from article 8, additional processing conditions prescribed in article 9 must be fulfilled[57].

3.1.2.3 Data processing principles

After the controller fulfills legal grounds for processing of personal data, basic principles of processing must be respected. These are prescribed in article 11 of the Data Protection Act. First principle can be referred as **the principle of lawful processing**[58]. This means that the personal data is processed only when this is authorized pursuant to articles 8 and 9 of the

---

thority, or to enable the controller or third parties to whom the data are disclosed to protect a legitimate interest, except where such interest is overridden by the interests of the data subject .

[57] Sensitive personal data (cf. section 2, no.8) may only be processed if the processing satisfies one of the conditions set out in section 8 and

a) the data subject consents to the processing,

b) there is statutory authority for such processing,

c) the processing is necessary to protect the vital interests of a person, and the data subject is incapable of giving his or her consent,

d) the processing relates exclusively to data which the data subject has voluntarily and manifestly made public,

e) the processing is necessary for the establishment, exercise or defence of a legal claim,

f) the processing is necessary to enable the controller to fulfil his obligations or exercise his rights in the field of employment law,

g) the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where the data are processed by health professionals subject to the obligation of professional secrecy, or

h) the processing is necessary for historical, statistical or scientific purposes, and the public interest in such processing being carried out clearly exceeds the disadvantages it might entail for the natural person….

[58] Data Privacy Law: An International Perspective, L.A. Bygrave, Oxford Scholarship Online: April 2014 at pg. 146.

Data Protection Act. This principle is in fact adding additional weight to the articles 8 and 9, and it is restating their importance in making the data processing legal.

Second principle is that of **purpose limitation**. This principle is embroidered in both points b) and c) of article 11. These state that the personal data are used only for explicitly stated purposes that are objectively justified by the activities of the controller (which can also be referred to as **the principle of purpose specification**), and that are not used subsequently for purposes that are incompatible with the original purpose of the collection, without the consent of the data subject (can also be referred to as **the principle of finality**)[59].

According to preparatory work, controller must define the purpose of processing in a specific manner, as vague purposes (such as: "administrative tasks" or "commercial use" are not allowed). This means that there should exist a certain level of proportionality in danger for breach of data privacy rights, and precision of defining the purpose of processing. If the danger is high, the purpose must be defined more strictly.[60] There is also a demand that processing is objectively justified by the activities of the controller, but the preparatory work did not elaborate on this demand. But according to the Privacy Appeals Board's practice, the purpose of data processing must have close and natural connection with the activities of the controller[61].

As far as the principle of finality is concerned, it covers situations where the data is already collected (and most likely legally processed). But now, the controller will process that same data, for other purposes, i.e. other than those that were known, when the data is already collected. In this case, the subsequent processing must oblige to conditions from articles 8. and eventually 9[62]. (even though the consent of the data subject is only specifically mentioned in article 11 (c)). The fact that the data is already collected has no importance on the

---

[59] Supra note 58. at pg. 153

[60] Ot.prp.nr.92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven) Merknader til de enkelte paragrafene, Kappitel II, Til § 11.

[61] PVN-2014-04 – "Post i butikk" case

[62] If the data is considered sensitive data.

legality of the new processing, and new and independent analysis of legality (of the processing) will follow[63].

Next principle is the **principle of minimality**. It stems from article 11 (d) and provides that the data must be adequate and relevant in relation to the purpose of the processing. The expression that the data must be 'relevant' is marking the ceiling for data processing operations and it is pointing to unnecessary data, which cannot be processed[64]. This requirement is closely connected to the **principle of proportionality,** which will be closely discussed in the part which deals with the case law. The requirement that the data is 'adequate', is made by the legislator, so that the ground for processing of personal data must be as complete as the purpose of the processing requires it.[65]

Next principle is **the principle of data quality**. It stems from article 11 (e) and provides that the data is accurate and up-to-date. Article 11 (e) also stipulates that the data must not be stored longer than is necessary for the purpose of the processing, and that requirement is not *per-se* part of the data quality principle. But it is placed in this provision for a purpose, and that purpose is to make sure that the data that is incorrect (or outdated) is deleted by the controller at its own initiative. Articles 28 and 29 of the Data Protection Act already govern this area, and the controller must (at its own initiative or at request of the data subject) rectify inaccurate data, or delete data whose processing is no longer necessary. According to preparatory work to the Act, article 11 (e) is placing this duty on the controller, as Articles 28 and 29 are more oriented on giving rights to data subject to request rectification or deletion of this data[66].

Next principle is the **principle of data security**, and it stems from article 13, which provides that the controller and the processor shall by means of planned, systematic measures ensure satisfactory data security with regard to confidentiality, integrity and accessibility in

---

[63] Supra note 60.

[64] Ibid.

[65] Ibid.

[66] Ibid.

connection with the processing of personal data. Data system and measures must be documented and available to their employees. Even though it is left out of the article 11, preparatory work confirms that this is also a principle, which adds on to the article 11.[67] Data security must be ensured at all time, and this requires both technical and organizational measures. The law does not set out specific demands for data security, and it is dependent on the type of threats the data can be exposed to, in every individual case. Significant threats will typically require significant measures, before the requirement of confidentiality, integrity and accessibility is fulfilled.[68]

Confidentiality requirement means that the data shall be made inaccessible to those who are not authorized. This means that the data must be protected against unauthorized insight, e.g. during transfer, use or storing. Integrity requirement means that the data cannot be changed, either unintentionally, or by unauthorized persons. This requirement is different from the requirement for data quality. Accessibility requirement means that the data is accessible to authorized users, upon their need, in order to fulfill their tasks and duties. [69]

3.2 Case law

After reviewing the central legal provisions, and their interpretation through the preparatory work of the Personal Data Act, this chapter will discuss the case law of The Privacy Appeals Board, which shaped the interpretation of article 12.

3.2.1.1 Tysvær municipality case PVN-2006-7

The first case that discussed the use of fingerprints in the data processing perspective was the case PVN- 2006-7. This was the appeal of Tysvær municipality upheld by Lenovo Technology BV Norway, to the Privacy Appeals Board. The case illustrates nicely all the steps undertaken in analysis of personal data processing, starting from valid legal grounds

[67] Ot.prp.nr.92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven) Merknader til de enkelte paragrafene, Kappitel II, Til § 13.

[68] Ibid.

[69] Ibid.

analysis, followed by analysis of general processing principles, moving to the case on point.

In this case, the Tysvær municipality purchased a number of Lenovo notebook computers equipped with fingerprint scanners. The purpose of purchase was to increase the security against unauthorized access to sensitive data in the municipal data system. The employee of the municipality would scan their finger to the reader, and a 75 points template would be generated. In case of a satisfactory match, username and password would be automatically inserted. The Norwegian Data Inspectorate issued a decision prohibiting Tysvær municipality any use of fingerprints in connection with logging on to the computer system[70].

The first thing that was discussed in the case was the fact if there is a valid legal ground for processing, which in this case was consent. Even though consent in the employer/employee relationship is treated harshly than other types of consent in Norway[71], in this case it was taken as a valid legal ground[72]. This was followed by the analysis of general processing principles stemming from article 11 of the Personal Data Act. These were also fulfilled. Finally, use of fingerprints was discussed in detail[73].

The Privacy Appeals Board explained the procedure of registering the fingerprint, and forming of a 'template' which contains 75 points. According to them, this is too small of a number (of points) to regenerate an image of a fingerprint.

After this, the Privacy Appeals Board started finally discussing article 12, in its entirety. Firstly, it was pointed that the term 'means of identification' is unclear, and that this 'mean of identification' has to be unique. It can be used for both authentication and identification.

---

[70] The Privacy Appeals Board repealed the case in favor of the appellant.

[71] By default it is insufficient as a valid ground. See pg.7 of PVN-2006-7 case.

[72] Because it was up to the employees to decide if they will use the technology or not, and the decision (not to use it) had no negative consequences on their employment relationship.

[73] Since this was the first time to discuss the issue of fingerprint use, cases from Sweden and Denmark were also used for illustrative purposes in the decision. It was concluded that Swedish and Danish law don't have their article 12 i.e. similar provision and model does not exist in these laws respectively. They use instead the general rules for data processing that match rules from articles 8 and 11 of the Personal Data Act.

A conclusion was made that an ID number and a fingerprint cannot be compared, because the former is given (by the authorities), while the latter is personal property (physical trait). With the term 'clear'[74], the law aims at something more than the identification that is clear for a single system. The law aims at something more, meaning that the same means of identification can be used in more than one system. This is why fingerprint is 'clear mean of identification' as it can be used in more than one system. 'Template' itself is not a clear mean of identification. While an ID number can be used only for identification, fingerprint can be used for both identification and authentication.

Already in this case, the Privacy Appeals Board expressed its concern for regulating ID numbers and fingerprints in the same way, as it was done in the article 12. It was firstly critical to the lack of explanation in the preparatory work. Also, they pointed out that biometric methods for identification or authentication have developed since the law had been passed[75].

Two members of the Board had dissenting opinions on the use of article 12 in this case. According to them, if fingerprints were to be treated together with the ID number, then the lawmaker was aiming at the use of fingerprints which was similar (or same) as the use of an ID number[76]. Their opinion was not upheld by the majority of the Board. The entire Board took however the position that if the processing falls out of the scope of article 12, general data processing rules must be applied.

Finally, the Board discussed the two major demands of article 12: that of objective need for certain identification, and the one of necessity. The Board found that the demand for objec-

---

[74] From 'clear means of identification'

[75] It was pointed out that attempts have been made to amend the law, but with no success.

[76] This was, according to dissenting members, not the case here, since fingerprint will be used to verify that the right person is trying to log in to the machine. The same cannot be accomplished by ID number. They are also sceptical about the use of 'template'. According to them, it's not possible to establish one-on-one relationship between a 'template' and a physical person. That is why they are sceptical to the argument that the template is established with the help of fingerprint pattern, and that the registration procedure therefore contains processing of fingerprints. The law defines the term 'processing' as collection, recording, alignment, storage and disclosure or a combination of such uses. According to them, none of those occur, when fingerprints are converted to the 'templates'. That is why article 12 cannot be used at the present case.

tive need for certain identification is fulfilled, because the machines in question store data on third parties, e.g. social and health services related data. And it is because of that, i.e. the third party's right to confidentiality, that the objective need for certain identification exists. It didn't take long for the Board to reach this conclusion, and it was elaborated in two-three sentences.

The question of necessity took the Board a bit more time and space in the decision. Necessity, according to preparatory work, exists if other, less safe means of identification cannot be used e.g. name, address or customer number. The Data Inspectorate, in its decision (appealed decision in this case) found that username and password could be used, and that is why the necessity demand is not fulfilled. The Board did not agree, stressing out the flaws of use of username and password. According to the Board, username is often known, and it is password that is secret. Users usually write their passwords as they do not rely on memorizing them. They vaguely pointed to the Banking Appeals Board's practice. Here a number of examples exist on how unauthorized persons got in possession of PIN codes not belonging to them. If passwords are compromised, non-authorized persons have access until the password changes. Use of smartcards with a password has a higher degree of certainty, and smartcard can also be a clear mean of identification if it can be used in more than one system. But it can also be left, lost or taken from its user. The notebook machines in question shall be carried by the employees, and could be forgotten outside the premises.

The Board showed understanding that municipality will, in those cases try to find a system that is easy, safe and robust. Use of fingerprints, as a log in procedure for the notebook machines, that contain sensitive data on third persons, will provide a solution of desired safety. But the Board interpreted the preparatory work in way that if there must not exist a solution that does not imply the use of clear means of identification that gives the same level of safety. The Board disagreed with the Data Inspectorate that smartcard and password are such a solution, and therefore concluded that necessity demand was also fulfilled.

3.2.1.2 Oxigeno fitness case PVN-2006-8

In this case, Oxigeno Fitness – a gym in Oslo used fingerprint scanners in order to facilitate access control of the center. The Data Inspectorate forbid the use of fingerprints for access control to the gym, and they complained to the Board.

The Board first showed to a Danish case from 2004[77], where the use of fingerprints was found not to be proportionate with the purpose of processing, because the fingerprints were stored in a database, and not on the member cards.

When analyzing the case, the Board first turned to general conditions for processing and found that consent requirements, as a legal ground for processing, were fulfilled, since the members gave consent willingly, and they were free to choose the technology away. Also conditions of article 11 were found to be fulfilled (but without much elaboration on the point).

Discussing the application of article 12, the Board admitted that there exists a practical purpose on the use of fingerprints, since one needs not remember the password or member card, and it makes sure that the person is indeed a member. These were enough for the Board to conclude that there was objective need certain identification.

As for the necessity requirement, the Board found that the gym can use other and less secure means of identification, that would fulfill their needs. Simple access to the center by its members and access control by the owners are good reasons, but they were not enough for the Board. Since there was possibility to use other methods, that did not include the use of safe means of identification, the Board decided that the necessity requirement was not fulfilled, and did not upheld the appeal.

3.2.1.3 Oslo trimsenter case PVN-2006-9

In this case, Oslo Trimsenter – a gym in Oslo used fingerprint scanners[78] for access control of the center. Upon registration, the members voluntarily scanned their fingerprints which were converted into a template, that was stored in a database. Members who chose not to consent to use of fingerprints were registered manually by the staff at each visit[79]. The Data

[77] Case of the Danish Data Inspectorate 2004-219-0208 from 26.11.2004

[78] Ident X sertices solution, like the one used by Oxigeno fitness.

[79] Only two out of 500 members opted out.

Inspectorate issued a decision forbidding such practice, and Oslo Trimsenter appealed the decision to the Privacy Appeals Board.

The Privacy Appeals Board went on to conclude that the requirements of articles 8 and 11 were fulfilled, without much of elaboration on the matter. The only thing that was mentioned was that, due to the existence of a choice (possibility to opt out of the use of fingerprint technology), the members consent was legitimate.

Here, the Board stressed out that 'clear mean of identification' must be usable in more than one system. They singled out KID number (customer identification number) as an example of a mean of identification (of a customer) in only one database (or a system), and concluded that KID is not 'clear' mean of identification because of it.

The Board concluded that there is a need a objective need for certain identification in this case, because the use of fingerprints instead of a member card is simpler, more practical and user friendly. One needs not remember to carry a member card.

However, it found that the necessity requirement is not fulfilled. It was not satisfied with the argument that the use of fingerprints give members a simple access, and that it gives the center a good overview over access itself. The Board stressed that something more is required. There had to be lack of solution that would give same level of safety, but that did not use a clear mean of identification. If that solution existed, the necessity demand would not be fulfilled. Since such solutions existed, the Board decided against the appeal.

3.2.1.4 Esso Norge case – PVN-2006-10

In this case, Esso Norge – an oil company, seeked license from the Data Inspectorate, in order to process personal data (fingerprints) in relation to access control for four of its oil depots. The employees who would consent to use of the fingerprints would fill out a consent form, and a scanner would be place at the facilities'' entrance. The use of fingerprints would ensure that only authorized personnel can access the facilities. The Data Inspectorate refused to give such license and ordered that any use of fingerprints stops immediately. Esso Norge appealed to the Board.

The Board concluded that requirements from articles 8 and 11 are fulfilled. Consent was used as a legal ground for processing in this case, and it was found to be valid by the

Board. This because it was done on voluntary basis, and employees had a real alternative in the combination of employee card and PIN code.

In this case, the employee card is used for identification of the driver. Driver would swipe the card and authentication occurs either by the use of PIN, or by the use of fingerprint. If the fingerprint is used, once the driver swipes the card, the system automatically chooses a template from the database. The two templates are then compared and access is granted or denied.

The Board concluded that requirement of objective need for certain identification was clearly fulfilled in this case. The aim of the measure was that only trained personnel can have access to oil depots.

The requirement of necessity however, took them more energy. They assumed that the use of fingerprints was made on the basis of free will of the employees. If there was a free will, there had to be real alternative. They followed to conclude that the requirement of necessity is central to the application of article 12. And if there is alternative, so logically, there cannot be necessity. Such interpretation, according to the Board, would exclude consent as a valid ground for processing in cases under article 12. And this would be against the purpose of the Personal Data Act.

That is why they stated that under article 12, the question that is relevant is if the solution that is chosen provides necessary safety for identification. Here, the solution must be evaluated in its entirety. Free willingness is therefore evaluated in relation to individual employee (data subject) while the necessity of use of clear means of identification is evaluated in relation to necessity of establishing of necessary safety for the entire system. This way, consent can be used as a valid ground for processing also for article 12.

Even though other means of identification and safety measures exist such as guards, high fences and walls, the oil storage facilities require a high level of safety, where great danger exists, should unauthorized access occur. Unlike REMA 1000 case (discussed below) the purpose of the measure is not surveillance, but a desire for safe workplace where the facilities can be considered dangerous. This is in everyone's interest (drivers, employees, employers and the society).

But this is not enough in itself. Additionally, other solutions that do not assume use of clear means of identification (and which provide same level of safety) must not exist. In the current situation, the Board found that they do not exist, and the appeal was upheld.

3.2.1.5 REMA 1000 case – PVN-2006-11

In this case, REMA 1000 – a supermarket chain, used a fingerprint processing system in its terminal which registers employee's arrival and departure from work. The employees would type in their employee ID and scan a finger in order to register for work. The Data Inspectorate received a tip from the employees and issued a decision forbidding REMA 1000 use of such system. REMA 1000 appealed the decision.

In this case, it was not the consent but the fulfillment of a contract to which the data subject is party, that was used as a ground for processing. The Board found that it was valid, since REMA 1000 used this system to pay the correct amount of salary to their employees (which received salary on hourly basis). Here as well, general principles of data processing from article 11 were abided to, and the Board didn't elaborate further on that matter.

The Board referred here to Esso Norge case, and stated that article 12 is applicable in situations where authentication occurs after identification took place. Article 12 thus covers situations where fingerprint authentication is one part of a system for secure identification.

On fulfillment of two cumulative conditions of article 12, the Board firstly mentioned that the whole idea of this system was to prevent abuse where the employees would share their IDs and PIN codes, and would help themselves by cross-registering, so that they would receive payment even if they came late (or never came to work at all). Prevention of misuse was enough for the Board, to find that the objective need for secure identification requirement is fulfilled.

As for necessity requirement, the Board was skeptical to the use of this method, as it showed an unnecessary suspicion of the employees by the employer. This was found to be a stricter means of control, which sends the signal that the employees cannot be trusted. Since other methods were available to REMA 1000, the Board decided that the necessity requirement was not fulfilled, and the appeal was not upheld.

3.2.1.6 Visma Retail case – PVN-2011-11

In this case, Visma Retail wished to use fingerprint biometric system to perform age control at a self service convenient store. They wished to introduce this system at the university campus, where the customers were to buy goods at a convenient store with no staff. When purchasing goods that require certain age (e.g. cigarettes or beer) customers could not complete purchase, and a person in charge of the store would come to the automatic cashier and ask for an ID. Additionally, it was possible to register the shopper, and in the next purchase of such goods, the shopper would use its fingerprint to verify his age. The Data Inspectorate advised the complainant that this solution was against article 12 of the Personal Data Act. Visma Retail complained than to the Board.

The Board explains in detail the difference between authentication and identification in this case. Identification, according to them, is about connecting a clear identifier to a determined resource (which can be a physical person). Authentication presumes implies that a certain (information) system is set up in way to confirm (or deny) if a statement is correct. Identification makes it possible to collect, store and connect together information about an identified object across systems. It can be accomplished regardless the fact that the information is correct or incorrect. Authentication is a phenomenon that relates to the truth of a certain claim. The Board set out examples of such claims:

1. I have the right of access to resource X.
2. I am over 18.
3. This person can clearly be identified by ID number: 01010012345.

The Board reached a conclusion that these two events must be considered separately, and that they have an impact on how to understand article 12. Out of those three questions, only the third one actually deals with identification. The first two can occur without any means of identification. One needs not know identity, in order to determine if a person has certain rights or not.

In the current case, the Board could not conclude that there is identification in question, or that the fingerprint is used as a clear mean of identification. The use of fingerprint is limited to the purposes of answering the question if the customer is old enough to buy the goods at stake. Therefore, this was the question of authentication.

The final point of the Board was that the solution of Visma Retail does not include processing of personal data at all. This was based on understanding that the template is used for pure authentication (or verification) and not identification. The things that are registered are: date of birth, template and a randomly generated number to be a key for the database (to connect date of birth with the template). It is also possible to use YES/NO statement instead of the birth date. This whole idea is made on the statement that the template cannot be reversed to a fingerprint.

The Board upheld the complaint, since there was no use of personal data, and therefore, Personal Data Act was inapplicable.

3.2.1.7 Fitness 24Seven case – PVN-2011-12

Fitness 24Seven established two gyms in Oslo in 2011, and the Data Inspectorate received an email where they were notified that gyms require use of fingerprints in order to enter the gym. Gyms were open 24/7 and were staffed only from 12 AM to 7 PM Monday-Friday. Customers would receive member cards, and on those cards (and only on those cards) a member's fingerprint was stored[80]. The customer would swipe the card, enter the first door and then swipe the card again, but this time she also needs to scan her fingerprint in order to enter the gym. The system was set up in way that it compares the template obtained at the scanner with the template stored in the card. The card would be synchronized with the payment system. If the membership fee is paid, the first door is opened. If not, the member can't reach the fingerprint scanner at all.

The Board found that this was the case of authentication (verification) and not identification. They could not see how the registration of a fingerprint template in a customer's member card, or provision of fingerprint in relation to access control, is identification. The solution was such, that both card and finger need to be read (by the machine) and there would occur a matching process, but the fingerprint is not stored in a way that other people or systems could retrieve it. Template was only registered in the card.

[80] Customers consented to the use of fingerprints (but it was not clear if they had any alternative, since without the use of fingerprints, they could enter the premises only from noon until 7 PM on workdays).

Since the process was made in order to match the card with the owner of the finger, there is no identification. Therefore, article 12 could not be applied in this case, since processing is not undertaken to accomplish "safe identification" as article 12 prescribes.

In a way this system works, it is not possible to reverse the template to a fingerprint. When the fingerprint is scanned, the machine can only confirm or deny if the person is the owner of the card. But that is not a personal data, and cannot be connected to a certain individual (directly or indirectly). The way the Board saw it, it was the number on the customer card that identified the customer, and not biometrics. Customer number is unique in this system, but not in others. That is why the identification that occurs is system specific, and does not go over it.

The Board upheld the complaint, and just as in the Visma Retail case, it excluded the application of Personal Data Act to the case.

3.2.1.8 Conclusion

As it can be seen, data protection rules governing the use of fingerprints in Norway are twofold. Firstly, general rules and principles apply (is there personal data, is the personal data being processed, is there a valid legal ground for processing and are the general principles of data processing abided). Secondly, rules specific to biometric data are being applied i.e. rules stemming from article 12. They consist of two main questions, if there is an objective need for certain (secure) identification, and if the method necessary to accomplish such identification exists. The Board has, through these seven cases, elaborated on almost every aspect, even though the most of the debate is centered on the question of necessity, where we got a good insight on the proportionality principle in Norway.

In all of these cases, the Board had no problem finding that valid legal grounds exist, and that the general principles of article 11 are respected[81]. The same can be said for the first requirement of article 12, that of objective need for certain identification. In order to fulfill

[81] There was no mention of the principle of data security in any of the cases, but that can be a question for the Data Inspectorate to deal with. Its importance today might even become greater due to emergence of cloud computing and 'identity-as-a-service' cloud services that are available on the market.

this requirement, it is enough that the measure is e.g. protecting interests of third parties (e.g. confidentiality of their data), or that the measure contributes to practicality e.g. eliminates the need to carry member cards, or remember passwords, or that the measure precludes misuse of certain rights e.g. password sharing between employees. Seen this way, almost every measure will be able to fulfill this first requirement, but same cannot be said for the requirement of necessity.

The requirement of necessity is in the core of **the principle of proportionality** in the processing of personal biometric data. The case law of the Board has given us a lot of material to better understand it. As Yue Liu correctly points out, the Board is using both the traditional interest-balance test, as well as the least drastic means test for evaluating necessity of the application at stake[82]. But these seem not to be separate tests, but two parts of one test. The Board is in all of the cases raised the issue of the least drastic means test, and it was bound to do so by the preparatory work of the Personal Data Act[83]. But it seems that it also contains interest-balance test. The Board seems to evaluate other, less drastic, means by looking at the interests that are being protected. That is how the use of fingerprints was allowed in Tysvær commune case, just as it was allowed in ESSO Norge case. In both of these cases, there seems to be a strong influence of interest-balance test to the least drastic means test. And one could argue that the use of fingerprints would have been prohibited, if the Board looked only to the least drastic means test, as it was bound by the preparatory work. But these are not the only two things one most look at when it comes to the principle of proportionality. The Board has made it clear that it will also look at the way the technology is used, and this was especially important in terms of where the template was stored. This was clearly illustrated in the Oxigeno fitness[84] case, where the Board inserted a reference to the Danish case from 2004, where the data is stored in a database, and not on the card. It was clear from this, that the Board does not prefer storing information in central

[82] The principle of proportionality in biometrics: case studies from Norway, Yue Liu, Computer law & security review, 2009 at pg. 249.

[83] See Tysvær commune case, PVN-2006-7.

[84] And also in Fitness 24Seven case. PVN-2011-12.

databases, and that such use would most likely be disproportionate to the purpose of processing.

The case law also taught us about the importance of distinction between identification and authentication[85]. In Visma Retail case, the Board found that the template[86] is used for pure authentication, and not identification. Given that it was the matter of authentication, and the template cannot be reversed into fingerprint, article 12 did not apply (nor did the entire Personal Data Act), as there was not personal data that has been processed. Perhaps more surprising was the decision in Fitness 24Seven case. Here, the Board found that it was a matter of authentication, and not identification, since the process was about matching a fingerprint with a card – verifying that the card belongs to the person swiping it[87]. Thus, article 12 did not apply to authentication at all.

[85] Sometimes the term verification is mentioned in the cases, having the same meaning as the term authentication.

[86] It is important to note that the Board discussed the use of template, and not fingerprint for authentication.

[87] But one must keep in mind that ESSO Norge case also had similar principle, and here the Article 12 applied. It could mean that the cases from 2011. set out new interpretation, putting aside earlier distinctions between identification and authentication. Authentication now, seems to avoid application of article 12, and most likely, entire Personal Data Act (as in Visma Retail case).

4 IV TECHNOLOGICAL DEVELOPMENT AND NORWEGIAN RULES

4.1 Fingerprint regeneration

The possibility to regenerate a raw image of the fingerprint from the template was introduced in earlier chapters. This part will discuss more closely possibility for such a thing, as well as its legal implications for the current interpretation of the Norwegian rules.

4.1.1 Is it possible to regenerate an image from the template?

This question has been asked many times even before the first line of cases emerged in 2006. Already up to 2005, we got 2 methods for reversing 'templates' into images, first being that of C.J. Hill from Australian National University in 2001[88] (Image 3) and second being joint effort of Arun Ross, Jidnya Shah, and Anil Jain in 2005 and furthered in 2007[89] (Image 4).[90]

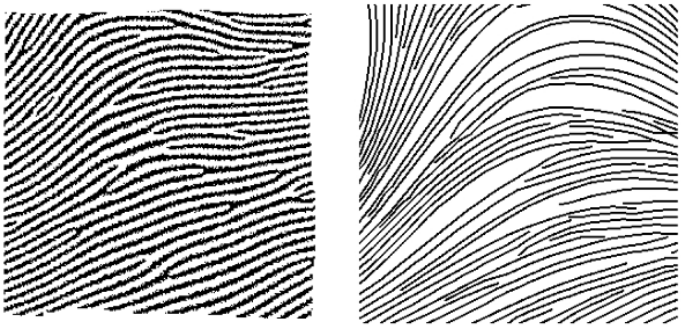

Image 3. Results of C.J.Hills reconstruction from the template, where the real fingerprint image is on the left, and on the right we have a result of the reconstruction (regeneration) that is still able to fool the system.

[88] Risk of Masquerade Arising from the Storage of Biometrics, , Hill C.J., Bachelor of Science Thesis, The Department of Computer Science Australian National University, 2001.

[89] Toward Reconstructing Fingerprints from Minutiae Points, Ross A.A., Shah J. and Jain A.K., in Proc. SPIE Conf. on Biometric Technology for Human Identification II, 2005. and From template to image: Reconstructing fingerprints from minutiae points, Ross A. IEEE Transactions on Pattern Analysis Machine Intelligence,vol. 29, no. 4, , 2007. at pg. 544–560

[90] Images (3,4 and 5) are taken from the Handbook of Fingerprint Recognition, D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Springer-Verlag London Limited 2009 at pg 381.

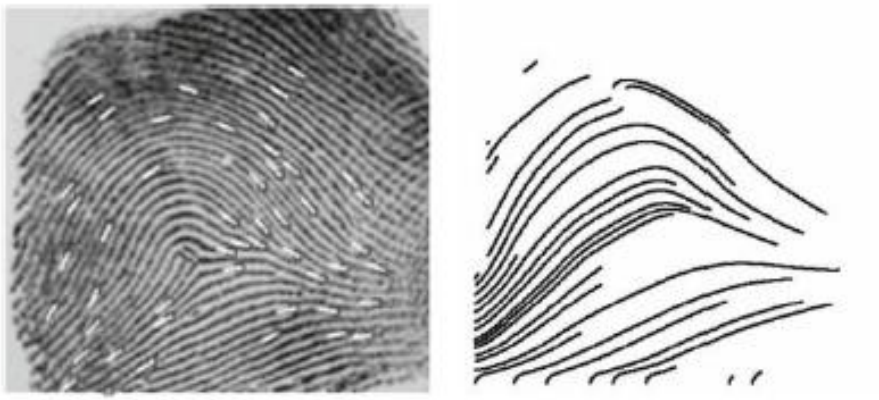

Image 4. Results of the joint effort (Ross, Shah and Jain) from 2005&2007. Even though the results are not similar to the eye of the layman, they are still able to fool an automatic system[91].

In 2007, Raffaele Cappelli from University of Bologna, with three other scientists[92], managed to obtain an average percentage of successful attacks of 81%, against nine fingerprint systems, even when these systems were tuned to operate at a high security level[93]. The visual result of the Cappelli method is shown in Image 5.

Image 5. This 'template' to image reversal (on the left we have the real fingerprint and picture on the right is regenerated image using Cappelli method) is visually very similar and it can easily fool the machine.

[91] Ibid.

[92] "Fingerprint image reconstruction from standard templates," Cappelli R., Lumini A., Maio D., Maltoni D., IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 29, no. 9, pp. 1489–1503, 2007.

[93] Supra note 91.

Apart from these three methods, others have attempted to reconstruct fingerprint images, and latest of these was already introduced in the earlier chapters of this paper, which dates to 2014[94]. All of these show that, at least in theory, image reconstruction from the 'template' is possible. Of course, various methods exist, that would increase the security of the template, and biometric system as a whole. This can be done by using e.g. an encryption of the template[95] but as Jidnya Shah stated, absolute security does not exist and nearly all security system can be compromised[96].

Given all that has been stated, one could answer that fingerprints can be regenerated from the 'template', and this answer might have serious consequences for the further interpretation of the Norwegian data protection rules.

4.1.2 How does it affect current interpretation of the Norwegian rules?

From the first case on use of fingerprints (Tysvær municipality case), the Board has made it clear that the template cannot be reversed back to the fingerprint image. But this finding didn't have much effect on the decision in the case. In all of the 2006 cases, the Board was clear that the template cannot be regenerated (e.g. in REMA 1000 case it was unknown how many minutia points the template has, but the claim of the appellant that it cannot be regenerated seems to be taken for granted by the Board). But in all of these cases, the Board focused more on the proportionality principle than on other issues, and this finding didn't have much effect on the outcome of the case.

However, the same cannot be said for 2011 (decisions from 2012) cases. In the Visma Retail case, the Board stated that "it is not possible to reverse a template to a fingerprint[97]". Since reversal (regeneration) was not possible, the Personal Data Act was inapplicable in

---

[94] At page 10. of this paper, I mentioned Amminaidu and Sreerama Murithy's method of fingerprint reconstruction.

[95] Can images be regenerated from biometric templates, Adler A., Biometrics Conference, September 2003.

[96] Reconstruction of Fingerprints from Minutiae Points, Shah J.A. Master thesis - Lane Department of Computer Science and Electrical Engineering, West Virginia 2005.at pt. 73.

[97] Page 6 of the decision, last paragraph.

this case[98]. Conclusion that the template cannot be used to regenerate fingerprint was also used in the Fitness 24Seven case[99].

As we can see here, the Board seems to completely exclude the possibility of fingerprint regeneration from the template, without giving at least a benefit of the doubt to the fact that the scientists have managed to do so many times in the span of the last 15 years. And the consequences of this were enormous. In a matter of authentication, the use of fingerprints (so long they are converted into templates) will not even trigger the application of Personal Data Act. One might argue that this conclusion is wrong.

If we are generous in our assumption that templates can, in most of the cases, be converted into fingerprints, than these templates would be personal data. Not only would they be personal data, but they could be 'clear means of identification', as they would be usable in more than one system (as they would be, at least in theory equal to fingerprints). Even though the templates were used as the means of verification in both of the cases, they would still be able to identify the holders of the fingerprint, and most likely would fall under the scope of article 12[100]. Thus, this assumption would make the outcome of both of these cases completely different.

Perhaps, in both of those cases, the templates could not be converted in fingerprints, but what surprises me the most is the fact that the Board was quick to reject such possibility[101].

---

[98] The facts of the case, as well as the analysis of the Board was given in the earlier chapters. Note that the Act as a whole was inapplicable, and not Article 12. This was due to the fact, that there was no personal data involved in the case.

[99] Also in this case, the same conclusion is reached – Personal Data Act is inapplicable, due to the fact that there was no fingerprint images involved.

[100] It would be interesting to see how the Board would react if the raw images instead of templates were used in these cases. In both of these cases, templates were used for authentication, and in Visma Retail case the Board emphasized this fact. I do believe that the Board would use article 12 in this hypothetical scenario, since the central point of its elaboration of the decision was the non-identifiable nature of the template.

[101] Even though the Board could mean that the fingerprints could not be regenerated only in the cases they resolved (based on the facts of the case), everything points to conclusion that they meant it generally. It was repeated as a general statement, and further general conclusions were made based on those statements. This was not decided under Facts of the case, which is additional argument that the Board meant it to be a general statement.

Another reason for skepticism about these decisions is the exclusion of application of Personal Data Act to both of these cases. This was related to the fact that the fingerprints could not be regenerated, but one could still argue (even if that was true given the specific facts of the case) that there was at least a processing of personal data[102].

According to preparatory work to the Act, fingerprints are personal data. The key point here is the term 'processing', which is defined as 'any purposeful use of personal data, such as collection, recording, storage and distribution or a combination of such methods of use"[103]. From the wording of article 2(2) of the Act, it seems that the list is not a closed one, and it is just an exemplary one. The central question would, in that case be: "How does one define the operation of scanning one's fingerprint and converting it into template?" If the fingerprint is personal data, which is quite clear from the Norwegian point of view, what is fingerprint scanning and conversion?[104] Data Protection Directive[105]has a far more extensive list of operations, used as examples of data processing operations, and these cover, among others: collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, etc. Fingerprint scanning is at least combination of collection, adaptation or alteration, recording and storage (in the enrollment stage) and collection, adaptation or alteration, retrieval and consultation (in the recognition stage). If we go back to the Norwegian definition, we can see that the use of fingerprints (both for identification and authentication) is a personal data (fingerprints) processing operation. This operation is performed with a certain purpose (e.g. access control or age verification), and it is done by

---

[102] This means that at least the general rules of the Personal Data Act have been applicable. Best case scenario would mean that article 12 was also applicable, as elaborated in the preceding paragraph.

[103] Supra note 52.

[104] The same applies for both enrolment and recognition stages. It goes without saying that the means for scanning and conversion of fingerprints are electronic, so according to article 3(a) the Personal Data Act is applicable from this aspect.

[105] Supra note 3. It is important to note that The preparatory work (Supra note 52.) confirms that the provision of the Personal Data Act related to data processing, is the same as the corresponding provision of the Data Protection Directive, with the only difference that the Norwegian provision has a simpler design. This should be an argument to use Data Protection Directive in order to interpret the Norwegian provision.

electronic means. This jointly means that such operations are falling under the scope of the Personal Data Act, and that they should be scrutinized under it. If not under article 12, which is only a specific mean of regulating use of fingerprints, then under general data protection rules and provisions of the Personal Data Act[106].

4.1.3 Conclusion

The fact that fingerprints could be reversed from 'templates,' makes a colossal difference in the application of the Norwegian data protection rules, and their current interpretation, given the case law of the Board. This would require a more detailed inspection of the biometric system from the Data Inspectorate, where they would have to look at the regeneration possibility on a case-to-case basis. All this would be necessary, in order to determine if there is personal data at stake (and if those templates are 'clear means of identification).

Of course, one has to keep in mind the workload of the Inspectorate, and see if it is practical (or even possible) that such detailed inspection is undertaken in each individual case. In all fairness, that would probably be the first thing parties would attack in their appeal to the Board. That is why it would be important for the Board to acknowledge the possibility of reversal in some of its next cases.

Of course, one cannot be satisfied with the fact that the Board has *de facto* separated identification and authentication completely, where pure authentication would fall out of the scope of the Act. Even if it is impossible to regenerate a fingerprint (and I have shown that it is not), it can still be argued that there is personal data that has been processed. Once the

[106] Additionally, it is important to note that templates alone, could be regarded, at least in some circumstances, as a personal data. This would mean not only clear situations like ESSO Norge case, but also some other limbo cases between ESSO Norge and Fitness 24Seven. As I already elaborated on the chapter on central definitions of Personal Data Act, personal data is "any information that may be linked to a natural person". The preparatory work of the Act defines natural person as the person that could be directly or indirectly identified, e.g. with the help of the name, id number or a physical trait. Additionally, even anonymized data can be personal data, if there are references or other linking points that would make the identification possible. And it's already explained in this paper that even the encrypted data can be personal data, if someone can make this data readable and identify persons to whom the data relates to. These arguments could be used to support the fact that 'templates' could be considered personal data, in some circumstances. Through templates, users could be identified indirectly by the operator of the system, since one can observe templates as anonymized (and probably encrypted) fingerprints.

finger is placed on the scanner, and the scanner started processing the image, we are processing personal data, and that fact should be enough to apply at least general data protection rules to the case. Perhaps the circumstance have been different at the time the decisions have been made, but today, with biometrics going into cloud and going mobile, fingerprints should be protected at any cost.

4.2 The Cloud

The novelty brought to us by the introduction of cloud computing is that the users don't need their own infrastructure (or software) in order to facilitate biometric (and other) solutions. This is mostly used by the businesses that only need access to internet and some basic hardware in order to benefit from the services provided in the cloud. National Institute of Standards and Technology (NIST) defines cloud computing as 'a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.'[107]

In order for one system to qualify as a cloud computing system, it has to fulfill certain criteria, as defined by the NIST. One of those criteria (the one of specific interest to data privacy) is that there is a resource pooling, which means that the provider is using a multi-tenant model and that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (country or even city). Typically we have three basic levels of service, where the provider is offering software, infrastructure or platform as a service[108].

---

[107] Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf at page 2. last visited on 31/10/15 at 12:16

[108] Ibid.

Basically, in order to qualify as a cloud, a service needs to be on-demand self service, with broad network access, and a measured service with rapid elasticity.

From the perspective of biometrics, all of these three levels can be used. Software as service is used when the provider is offering access to its biometric processing software[109]. Infrastructure as a service can be used when the provider is offering its virtual servers, storage or networks (where the cloud infrastructure is connected to the physical devices at the customer's premises). Platform as a service is used primarily in matters of identification, and it is not used as often as the first two components.[110]

4.2.1 Biometrics as a service

The previous subchapter introduced the cloud computing and briefly elaborated how it is used in the field of biometrics, while this subchapter will illustrate how a biometric system works in the cloud.

It is relevant to understand that we have two different types of biometrics as a service: authentication and identification. These logically depend on what kind of functionalities stand behind these systems. Both of them usually combine infrastructure and software as a service models, where the user (organization or private user) installs necessary scanners, and with the help of internet connection is using the software solutions as well as servers and/or storage from the service provider. This means that both the enrollment and the recognition stage occur in the cloud. This is illustrated by Image 6.[111].

[109] It can be fully developed software, or a software platform which can be customized to a certain point.

[110] *See* Biometrics in the cloud - What does cloud computing mean for biometric systems? R.Das, Keesing Journal of Documents & Identity February 2013, pg. 21-23

[111] Biometric Authentication as a Service for Enterprise Identity Management Deployment - A Data Protection Perspective, C.Senk and F.Dotzler, 2011. at pg. 2.

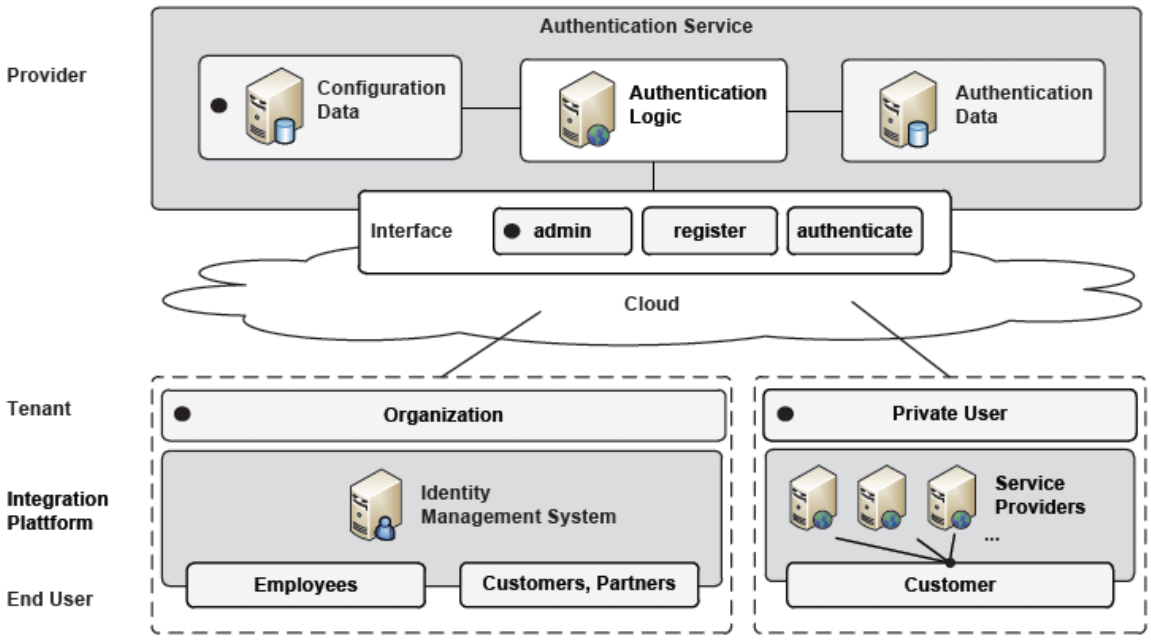

Image 6. Illustration of biometrics as a service model (authentication system).

Maybe the best illustration on how the system works would be the use of a real life solution. ImageWare Systems Inc has developed GoCloudID service, which is one of the leading services in the cloud, which is employing biometrics[112]. The process is, just as in any biometric application outside the cloud, twofold. In the enrollment stage, the fingerprint is scanned and sent to the company along with the identity information, and then the biometric information is stored in the cloud the company is using. There, biometric information gets an unique identifier, and the ImageWare Inc's systems (GoCloudID) stores this data. The identity of the end user is not known to the cloud provider, but the biometric data, on the other hand, is. This is illustrated by image 7[113].

[112] http://gocloudid.com/about/what-is-gocloudid-com/biometrics-as-a-service/ last visited on 02/11/15 at 09:55

[113] Ibid.

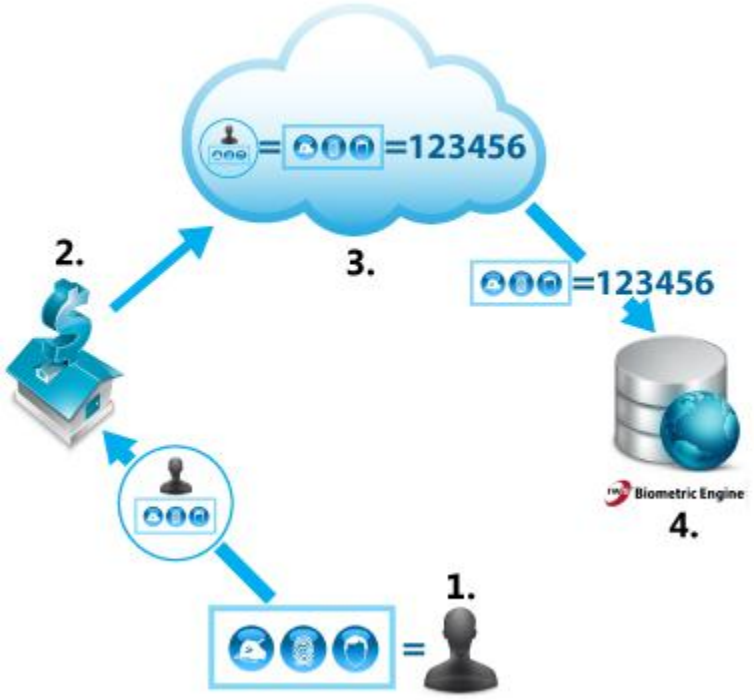

Image 7 Enrollment in the cloud (GoCloudID system).

In the recognition stage, the user requests access to the company[114], and she sends credentials and scans her fingerprint in the authorization stage. Credentials are confirmed already at the company, and the biometric data is traveling to cloud and forwarded all the way to the GoCloudID provider, in order to confirm or deny biometric identity. This information is then sent back to the company and finally the end user gets a response (usually in the form of finishing the transaction or cancelling it). This is illustrated by Image 8[115]. In GoCloudID system the templates are held in a database. Here, it is the token, that is issued at both stages (at the moment of template generation) is used to locate the template in the

[114] This system is pioneered by banks, especially in the area of credit card banking. In order to authorize the use of credit card (single purchase) the user will request access to the company, by stating his ID, or password and use of biometrics. This usually happens after the card is swiped, by using his smartphone.

[115] Supra note 113.

database, and the operator of the service does not have knowledge on the identity of the holder of the fingerprint (from which the template is generated)[116].

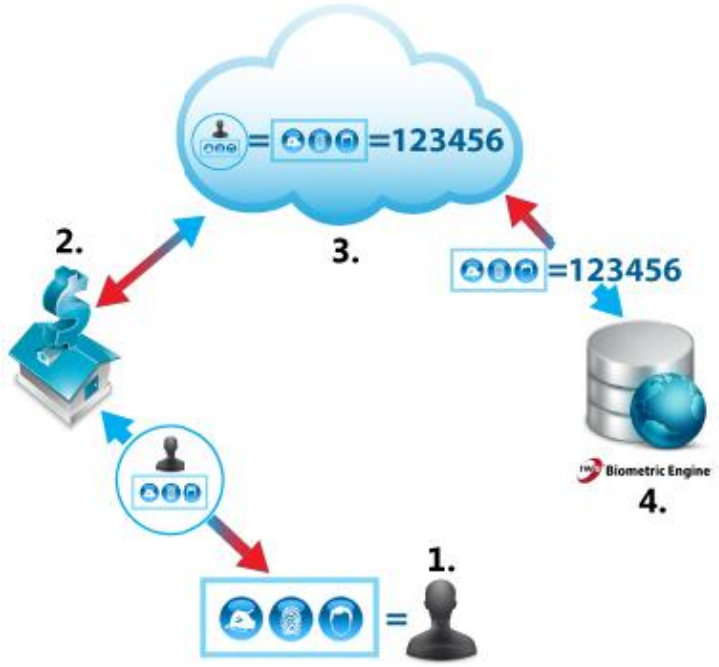

Image 8. Recognition stage in GoCloudID.

[116] An example: suppose an individual wishes to gain access to her personal bank account. She is asked to verify his or her identity by the bank. The bank provided a fingerprint reader in order to retrieve the biometric data from said individual. Biometric client captures biometric data which then collected and formatted to be used in further steps. At the same time, using the individual's ID, a unique identifier, also referred as "token" was retrieved from the bank's database and associated to the individual. Token and biometric data were then sent to the anonymous biometric verification server, referred as the anonymous sector in the preceding description over a suitable computer network. Query router located in the anonymous sector receives the token and biometric data as SOA calls and processes the request. Query router assigns the verification task to one or more query engine(s). Query engine(s) then using a query search engine located template(s) by matching token with index of token contained within a template database. Automatically after template(s) were matched, score(s) were assigned and sent back to query router. Query router combines the scores score(s) and sends one SOA response back to the bank, wherein an end user application receives the score(s) and interpreted as a successful verification, hence granting access to the individual. More can be found on USPTO Patent Database where the ImageWare Systems, Inc's patent number 8,887,259 of November 11, 2014 is described.

4.2.2 How does it affect current interpretation of the Norwegian rules?

Given the emergence of the cloud, and its symbioses with the biometric systems, it is clear that there are a couple of problematic areas from the perspective of the Norwegian data privacy laws. First problem is the multi-tenant architecture that is one of the core characteristics of the cloud. Multi-tenancy is based on the fact that the cloud provider does not set up separate service instances for different tenants (users of the cloud services). They use (and customize) dedicated virtual partitions of the same system instead of using a dedicated system instance. Logically centralized service interfaces map single requests to the according tenant's partition. Of course, there is a clear separation of each tenant's data.[117] This multi-tenancy characteristic has implications on the status of templates in the data protection universe. If any user can use the same cloud service to generate templates, and if the way of generating templates is the same for every user (of every client using cloud services), then this would be one step towards the templates (if one accepts that they can be personal data[118]) being governed by article 12, as they would be susceptible to use in more than one system[119].

Another matter that could affect the data privacy laws is that the templates are generally stored in a database, and not in a token. As we can see from the GoCloudID system, bio-

---

[117] Supra note 112 at pg. 3.

[118] By using the argument that the controller has the possibility to identify the individual to whom the template belongs indirectly (through a token for example).

[119] This does not have to occur in every instance, but the possibility that it does should not be excluded. The same user can also use two different services and still undergo one process of template generation (two companies using same cloud software as a service). In the past 15 years we have had 7 cases on the use of fingerprints in Norway, and two of them used the same (IdentX) solution. Given the amount of patents in this area, it is not impossible that different services apply same 'biometrics as a service' solutions in Norway.

Recent research shows that 1,6 million Norwegians used mobile banking last year. Many have more than one bank, and have downloaded more than one application for mobile banking. Given the number of smartphones with fingerprint scanner, abovementioned scenario could be a reality, should the banks for instance, turn to the same cloud provider.

Link to mobilebanking research in Norway: https://www.fno.no/aktuelt/sporreundersokelser/dagligbankundersokelsen1/dagligbankundersokelsen-2014/16-millioner-nordmenn-bruker-mobilbank/ last visited on 25/11/15 at 13:59

metric data is held in a database. Other services are also aiming towards storing biometric data in the cloud, one of the most prominent ones being Apple's iCloud biometric application (that shall be discussed in the next chapter). This fact could most certainly affect the balancing test undertaken by the Inspectorate and the Board, in deciding if the principle of proportionality is respected. The Board clearly indicated this in Oxigeno fitness case that it might not be proportionate (by referring to a Danish case from 2004). The only problem with this is, what happens if pure authentication occurs, and templates are stored in the cloud database (if Visma Retail facts occurred in the cloud environment)? Would the Board still disapply the rules of the Personal Data Act? One can only assume that in that scenario, the Board would (should) be much more protective over biometric data, and much more restrictive for such processing.

These examples only illustrate the fact that the emergence of biometrics as a service (in the cloud) can affect current interpretation of data protection rules in Norway, and give it a completely new direction. Given the lack of control a company (using cloud services) has over the personal data, which is specific for cloud services, data protection rules and their interpretation must be adapted to this new situation.

4.2.3 Conclusion

With the emergence of cloud computing and with it biometric identification and authentication in the cloud, the scenario that existed with 'traditional' technologies has changed drastically. Lack of user control over data (both in terms of processing and transfer), where data is stored in a database, along with the problem of same code base for all customers, where software is configured not customized, are the main areas of concern in the current regime. It remains to be seen how will the Norwegian agencies interpret its rules when they encounter biometrics as a service, but most likely, we are about to see some changes. We might see different interpretation of proportionality principle, given the storage of biometric templates in a database on a server in 'God knows where'. Additionally we might expect different treatment of 'pure biometric authentication' when it occurs in the cloud environment, due to lack of user control or customization. Given the fact that the cloud is suitable for mobile solutions as well, and the emergence of smarthpones with biometric

scanners and access to internet, it will not be long before we encounter such cases in Norway.

4.3 Mobile outburst (and e-payment)

While the first two developments, described in previous subchapters directly influence the way personal data legislation is interpreted, this last development effects both the law and the politics behind the law. Up until 2014, biometric solutions used in private sector were in most instances, 'local' in their nature. This means that, in the majority of instances, the controller who implemented the system and used it, governed the equipment and the processing of data[120]. With the emergence of smartphones with fingerprint scanners, such as iPhone 6 and Samsung Galaxy S6 (two dominant models in Norway at the time of writing this article[121]), not only are people carrying a fingerprint scanner in their pocket/purse, but they can use it (smartphone with fingerprint scanner) to facilitate transactions. And if we logically assume that before, in the private sector, fingerprints were generally uninteresting for various types of abuses (it is hard to imagine someone using time and resources to attack the system and abuse fingerprints to enter a fitness studio, or to verify its age in order to get beer or cigarettes), different thing can be said now. Thieves have a very good incentive to abuse a biometric system, as it is monetary gain that will fuel their actions now.

4.3.1 How does it work?

A good example on how the system work is Apple's Touch ID. Touch ID is, according to Apple Inc, the fingerprint sensing system that makes secure access to the device faster and easier. When the user places its finger on the scanner, Touch ID scans and recognizes it, and the device unlocks without the use of a passcode. Security and privacy of the data on the smartphone is not the only thing Touch ID is securing. It can be used to confirm purchases in Apple's iTunes store, or it can be used to verify purchases elsewhere, using Apple

[120] As seen from the Tysvær kommune case, computers with integrated fingerprint scanners existed in 2006, but they weren't dominant on the market, and those who were purchased were mostly used for private purposes.

[121] http://www.dinside.no/tester/mobil last visited on 05/11/15 at 10:58

pay[122]. By using Apple pay, the user does not need credit card, but uses the smartphone to make purchases. **Images 9 and 10**[123] illustrate how the system works.

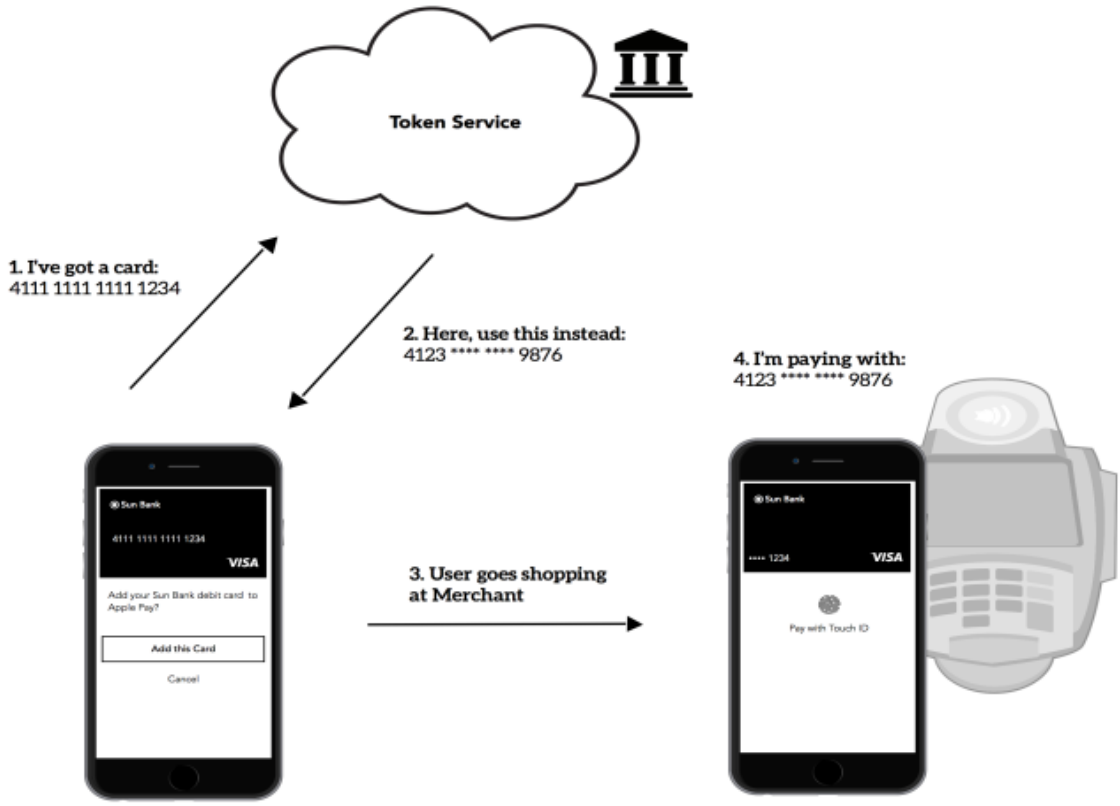

Image 9. Apple pay system – Smartphone communicates with the token service, which replaces a card number with a token generated number. The user is than placing the phone close to the terminal to make the transaction.

[122] Apple's iOS Security guide for iOS 9.0 or later, September 2015

[123] Images taken from: http://now.avg.com/three-reasons-to-be-happy-that-apple-pay-has-arrived-in-the-uk/ last visited on 05/11/2015 at 11:34

It is in the end of this stage where the user (smartphone owner) is using its fingerprint to verify the transaction. As it can be seen, the card is pre-registered in the system, and it is only the fingerprint that is required, in order to process the transaction. This is done by using Touch ID, which, according to Apple, is storing the fingerprint data is stored locally on the device, and never leaves the smartphone[124].

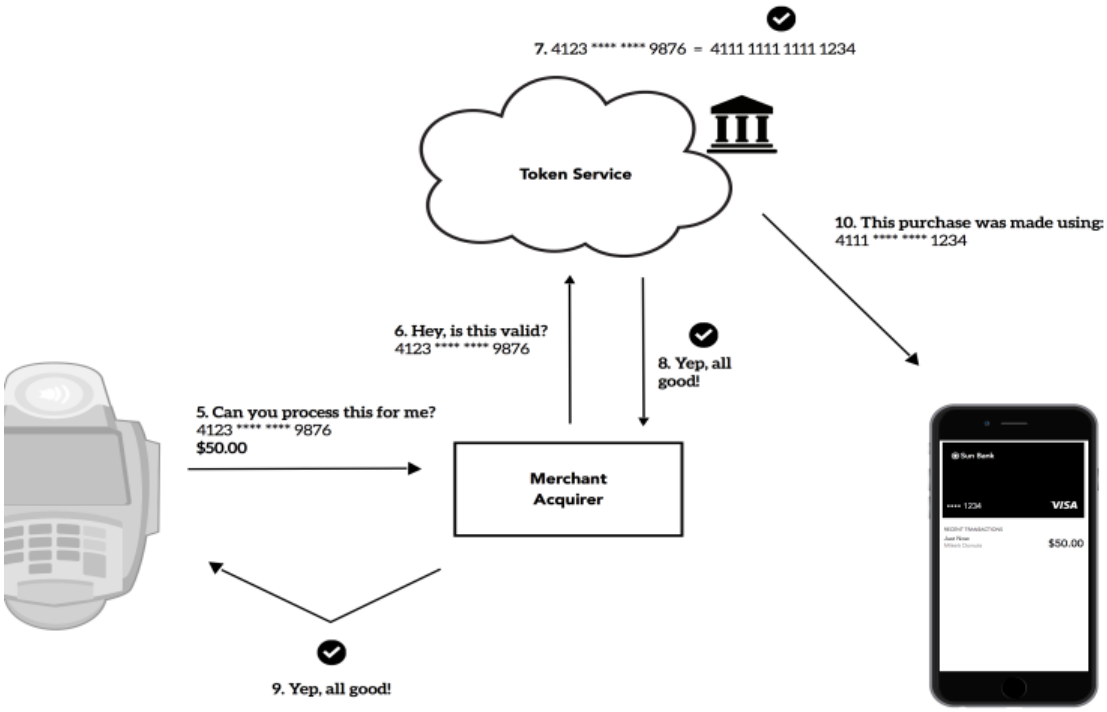

Image 10. The terminal is communicating with the token service which confirms that the holder of the smartphone is providing a valid card with sufficient funds, and the transaction is then confirmed.

As seen from these illustrations, we might be entering an era where we pay with our fingertips. One might say that this is an oversimplified statement, given the fact that one needs to

[124] https://www.nowsecure.com/blog/2013/09/19/the-security-of-your-fingerprints-thoughts-on-the-apple-touch-id/ last visited on 05/11/2015 at 11:44

register its card on its phone first, but still, the fact remains that fingerprint biometrics is starting to play much bigger role in monetary transactions (and in everyday life) than ever before.

4.3.2 How does it affect data privacy?

Apple claims that the fingerprint data never leaves the device, and remains in their A7 processor, as encrypted data[125]. However, Apple seems to be very open to the possibility of moving this data in the cloud. Already in 2013, Apple applied for a patent to the United States Patent and Trademark Office[126] to protect its method for synchronization of fingerprint biometric data via iCloud (Apple's very own cloud computing service). The core behind this patent application is that fingerprint data would be collected and processed by one device, sent to the cloud database as enrolment data. The user would then scan its finger on another device, and that data would be processed in this second device. Meanwhile, enrolment data would be downloaded from the cloud to the second device, and would be matched with the recognition data[127].

Whichever model is being used – whether centrally located biometric data, or biometric data in the cloud, we lack information about what happens to our biometric data. Currently we lack information on what happens to our data from unbiased sources[128], as we only have manufacturers explaining what happens to our data. Given the very nature of fingerprints, which cannot be replaced in case of abuse – unlike passwords and PIN codes, some interruption by authorities would certainly feel welcome. This is exaggerated by the fact that the European Central Bank, in its 'Recommendations for the security of internet payments' is advocating for the use of fingerprints, for strong customer authentication in internet pay-

---

[125] http://www.imore.com/how-touch-id-works last visited on 05/11/15 at 12:09

[126] Patent application number: 20150016697 filed before the USPTO under the name: FINGER BIOMETRIC SENSOR DATA SYNCHRONIZATION VIA A CLOUD COMPUTING DEVICE AND RELATED METHODS.

[127] Ibid.

[128] http://abgoode.blogspot.no/2015/02/the-impact-of-privacy-and-data.html last visited on 09/11/15 at 14:27

ments[129]. If we start using fingerprint authentication as a standard for internet payments, it will most likely be facilitated through our smartphones. And if this happens, we do just might need the Data Inspectorate to kick in.

4.3.3 Conclusion

With the current interpretation, from Visma Retail and Fitness 24Seven, fingerprint authentication system with the use of template escapes application of data protection rules. This means that every such payment authentication system would be beyond control of the data inspectorate. From reasons already explained above (template as a personal data, fingerprint scanning as processing of personal data, lack of control over data in cloud) it is of importance to set some sort of control to this payment authentication practice[130].

As we only have one set of fingerprints that can be compromised, the Data Inspectorate should have the ability to control how they are being used. One argument in favor of that is the recent 'fooling' of Touch ID made by a German hacker club, where a fingerprint of the phone user, photographed from a glass surface, was enough to create a fake finger that could unlock an iPhone 5s secured with TouchID. It was printed on a transparent sheet, smeared with pink latex milk, and placed on sensor (and unlocked the iPhone fooling it to be a fingerprint of its user)[131].

As the Data Inspectorate already has a mandate to protect the way our personal data is used, and as fingerprints are classified as personal data, it is a time to reconsider the interpretation set out in the last two cases of the Board (Visma Retail and Fitness 24Seven).

---

[129] European Central Bank - RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS Final version after public consultation, 2013

[130] Additional uses of fingerprint authentication on smartphone may emerge, and there should at least be a possibility for the Data Inspectorate to control them.

[131] http://www.imore.com/touch-id-fooled-not-hacked-lifted-fingerprint and

https://www.youtube.com/watch?v=HM8b8d8kSNQ last visited on 09/11/15 at 15:08

5 CONCLUSION

Technological development which occurred after the last decision of the Board in 2012, has affected drastically the area of fingerprint biometrics in private sector. Emergence and raise in use of fingerprint scanners integrated in smartphones alone raised the value of fingerprints as a personal data. In conjunction with it is the emergence of e-payment systems. Here the user is no longer required to use the PIN code (in some occasions card needs not be present either), but it is enough to scan the fingertip with the smartphone, and payment shall be finalized. With these two novelties alone, the need to protect fingerprints as personal data is more important than ever. But along with them, we have the emergence of cloud services, where the controller (user of cloud service) is using a multi-tenant architecture, and generally has lesser degree of control over personal data (as opposed to non-cloud based biometric systems). Finally, successful attempts are constantly made to create new methods of regenerating fingerprints from biometric templates. In the light of all these developments, the current interpretation of the Norwegian data protection rules (by the Board) is indeed inadequate. Even though the law might seem strict, especially with the relatively high threshold placed on the necessity requirement of article 12 (of the Personal Data Act), in reality, the Norwegian data privacy rules fail to protect data subjects privacy.

Firstly, there should be some space for re-discussing the position of 'templates' as personal data. The Board was clear that they do not qualify as personal data, but recent development in the field of fingerprint regeneration might point to the fact that in some (if not many) cases 'templates' are indeed a personal data. Given the preparatory work to the Personal Data Act, 'templates' could in other instances (even without regeneration) be personal data, just as anonymized and encrypted data can be personal data. With cloud computing, and its multi-tenancy architecture, 'templates' could in theory, even be scrutinized under article 12 as clear means of identification, as different systems using same cloud provider could end up having the same template.

Secondly, given the value of fingerprints (especially due to mobile and e-payment development) authentication should not be excluded from the application of data protection rules, so long as there is processing of personal data. Since fingerprints are specifically

mentioned as an example of personal data, in the preparatory work to the Personal Data Act, some control of such processing by the authorities should exist.

Finally, one can argue that in scanning a fingerprint, one does process personal data. Scanning a fingerprint on a smartphone integrated scanner is nothing but collection, adaptation or alteration, retrieval and consultation of personal data (fingerprints), and as such, it should be governed by the Personal Data Act. Even if article 12 is not used, general data protection rules should still apply, and the Data Inspectorate would still be able to control how our fingerprints are being used. This way, in case of biometric authentication systems, fingerprints would be treated as any other default personal data, and at least the general principles of data processing would apply.

To conclude, this paper shows that recent development has made the current interpretation of data protection rules (related to fingerprint processing in private sector) decrepit, and it is certainly desirable that the new cases emerge, where the Board would be able to update the interpretation in line with the current state of the art. Otherwise, a lot of personal data will be processed without proper supervision. Given the fact that fingerprints, once compromised, cannot be replaced, this might have serious consequences for the data subjects in the coming years (as everything points to the fact that fingerprints will be used more and more in the private sector with the development of technology).

6 Table of reference

Legal instruments

Lov om behandling av personopplysninger (personopplysningsloven)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Article 29 Data Protection Working Party's Opinion 3/2012 on developments in biometric technologies

Notat fra Datatilsynet – forslag til revisjon av personopplysningslovens § 12 og ny bestemmelse om bruk av biometriske data

Ot.prp.nr.92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven) Merknader til de enkelte paragrafene

NOU 1997:19 Et bedre personvern - forslag til lov om behandling av personopplysninger, Del III: UTVALGETS LOVFORSLAG MED MERKNADER

List of cases – Privacy Appeals Board

PVN-2014-04 - Post i butikk case

PVN-2006-7 - Tysvær municipality case

PVN-2006-8 - Oxigeno fitness case

PVN-2006-9 - Oslo trimsenter case

PVN-2006-10 - Esso Norge case

PVN-2006-11 - REMA 1000 case

PVN-2011-11 - Visma Retail case

PVN-2011-12 - Fitness 24Seven case

Case nr. 2004-219-0208 from 26.11.2004 of the Danish Data Inspectorate (referred to in PVN-2006-8 - Oxigeno fitness case)

Secondary literature

Privacy and Data Protection Issues of Biometric Applications, Els J. Kindt, Springer Science+Business Media Dordrecht 2013

Case Studies and Theory Development in the Social Sciences, George & Bennett, Belfer Center Studies in International Security 2005,

See Introduction to biometrics, Anil K. Jain, Arun A. Ross and Karthik Nandakumar, Springer Science+Business Media, LLC 2011

Practical Biometrics - From Aspiration to Implementation, Julian Ashbourn, Springer-Verlag London 2004, 2015

Fingerprint biometrics in the real world, Chris Trytten, Biometric Technology Today, June 2012.

Handbook of Fingerprint Recognition, D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Springer-Verlag London Limited 2009

Biometrics in the cloud What does cloud computing mean for biometric systems? Davi Ras, Keesing Journal of Documents & Identity, February 2013

Fingerprint Image Reconstruction from Standard Templates, R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, SEPTEMBER 2007

Fingerprint Reconstruction: From Minutiae, B. Amminaidu and V. Sreerama Murithy, Advances in Intelligent Systems and Computing vol 249, Springer International Publishing Switzerland 2014

The principle of proportionality in biometrics: case studies from Norway, Yue Liu, Computer law & security review, 2009

Risk of Masquerade Arising from the Storage of Biometrics, , Hill C.J., Bachelor of Science Thesis, The De-partment of Computer Science Australian National University, 2001.

Toward Reconstructing Fingerprints from Minutiae Points, Ross A.A., Shah J. and Jain A.K., in Proc. SPIE Conf. on Biometric Technology for Human Identification II, 2005.

From template to image: Reconstructing fingerprints from minutiae points, Ross A. IEEE Transactions on Pattern Analysis Machine Intelligence,vol. 29, no. 4, , 2007.

Fingerprint image reconstruction from standard templates," Cappelli R., Lumini A., Maio D., Maltoni D., IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 29, no. 9, 2007

Reconstruction of Fingerprints from Minutiae Points, Master thesis, Lane Department of Computer Science and Electrical Engineering, West Virginia 2005.

Can images be regenerated from biometric templates, Adler A., Biometrics Conference, September 2003.

Reconstruction of Fingerprints from Minutiae Points, Shah J.A. Master thesis - Lane Department of Computer Science and Electrical Engineering, West Virginia 2005.

Biometrics in the cloud - What does cloud computing mean for biometric systems? R.Das, Keesing Journal of Documents & Identity February 2013,

Biometric Authentication as a Service for Enterprise Identity Management Deployment - A Data Protection Perspective, C.Senk and F.Dotzler, 2011

Apple's iOS Security guide for iOS 9.0 or later, September 2015

Patent application number: 20150016697 FINGER BIOMETRIC SENSOR DATA SYNCHRONIZATION VIA A CLOUD COMPUTING DEVICE AND RELATED METHODS United States Patent and Trademark Office

Patent number 8,887,259 of November 11, 2014, United States Patent and Trademark Office

European Central Bank - RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS Final version after public consultation, 2013

Web pages

http://www.census.gov/popclock/ US Census Bureau's U.S. and World Population Clock, last visited on 30/09/15 at 12:09

http://www.identityone.net/BiometricTechnology.aspx last visited 30/09/15 at 13:04

http://webcusp.com/list-of-all-fingerprint-scanner-enabled-smartphones/ last visited on 05/10/15 at 11:06

http://www.dagbladet.no/2015/02/17/tema/dinside/aller/mobil/teknologi/37758810/ last visited on 05/10/15 at 11:10

http://www.elektronikkbransjen.no/Presse/Omsetningstall-og-presentasjoner last visited on 05/10/15 at 11:15

http://www.biometricupdate.com/201510/mastercard-rolling-out-payment-system-using-facial-and-fingerprint-recognition last visited on 07/10/15 at 11:58

http://www.innovasjonnorge.no/no/grunder/Grunderhistorier/finger-pa-framtiden1/#.VhTtMfntmko last visited on 07/10/15 at 12:02

http://www.biometricupdate.com/201509/tsi-and-trust-designer-develop-e-wallet-with-integrated-biometric-connected-device last visited on 07/10/15 at 12:09

http://www.biometricupdate.com/201509/payment-service-samsung-pay-goes-live-in-the-u-s last visited on 07/10/15 at 12:16

http://www.dinside.no/896430/nordmenn-foretrekker-bankkort last visited on 07/10/15 at 12:15

http://www.nrk.no/norge/onsker-et-kontantfritt-norge-i-2020-1.11830344 last visited on 07/10/15 at 12:20

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf last visited on 31/10/15 at 12:16

http://gocloudid.com/about/what-is-gocloudid-com/biometrics-as-a-service/ last visited on 02/11/15 at 09:55

https://www.fno.no/aktuelt/sporreundersokelser/dagligbankundersokelsen1/dagligbankundersokelsen-2014/16-millioner-nordmenn-bruker-mobilbank/ last visited on 25/11/15 at 13:59

http://www.dinside.no/tester/mobil last visited on 05/11/15 at 10:58

http://now.avg.com/three-reasons-to-be-happy-that-apple-pay-has-arrived-in-the-uk/ last visited on 05/11/2015 at 11:34

https://www.nowsecure.com/blog/2013/09/19/the-security-of-your-fingerprints-thoughts-on-the-apple-touch-id/ last visited on 05/11/2015 at 11:44

http://www.imore.com/how-touch-id-works last visited on 05/11/15 at 12:09

http://abgoode.blogspot.no/2015/02/the-impact-of-privacy-and-data.html last visited on 09/11/15 at 14:27

http://www.imore.com/touch-id-fooled-not-hacked-lifted-fingerprint last visited on 09/11/15 at 15:08

https://www.youtube.com/watch?v=HM8b8d8kSNQ last visited on 09/11/15 at 15:08