Personalized Pricing through Profiling

Wictor Björklund

Thesis in Legal Informatics, 30 HE credits
Examiner: Johan Axhamn
Stockholm, Autumn term 2017
Abstract
This thesis examines the legal aspects of using personal data for personalized pricing in light of the General Data Protection Regulation (GDPR). Personalized pricing is the practice of assigning a particular price to a particular person. The use of profiling technology and big data allows computers to harness great amounts of data and predict behavior. This development has made personal data a valuable commodity and brought forth a new regulation from the European Union (EU) regulating the processing of personal data.

Personalized pricing on a large scale is possible through using personal data to create profiles, estimating how much a person would be willing to pay, given his or her personal circumstances. Due to a growing use of the internet, sellers have access to more and more information of buyers. This information coupled with the technology to harness it creates an information asymmetry for the buyers.

Using personal data for profiling is a powerful tool for anyone wishing to extract information and patterns from large amounts of data. Its use therefore ranges from personalized pricing to credit ratings to suggesting music suggestions to fighting crime. Data may be gathered from various sources in various ways and used to find correlations, variations and even reveal future events by looking at earlier patterns. The use of personal data in this way poses a threat to the privacy of individuals and must therefore be regulated.

This thesis discusses the concepts of data profiling and personalized pricing as well as the GDPR. The intersection of technology, economy and law in the area of personalized pricing is therefore the main subject of this thesis while dissecting and discussing the phenomena and the regulation.

Keywords: personalized pricing, personal data, data processing, General Data Protection, Regulation, GDPR.
1 Introduction .................................................................................................................................6
  1.1 Background ...............................................................................................................................6
  1.2 Aim and Research Question ......................................................................................................7
  1.3 Definitions .................................................................................................................................8
  1.4 Methods and material ...............................................................................................................8
  1.5 Delimitation .............................................................................................................................9
  1.6 Outline ....................................................................................................................................10

2 Price Discrimination ....................................................................................................................10
  2.1 Degrees of Discrimination .......................................................................................................11
    2.1.1 Third Degree Discrimination .............................................................................................11
    2.1.2 Second Degree Discrimination ......................................................................................11
      2.1.2.1 Amazon’s Group Pricing ............................................................................................11
    2.1.3 First degree discrimination ...............................................................................................12
  2.2 Information asymmetry ........................................................................................................12

3 Profiling .....................................................................................................................................13
  3.1 How Profiling Works ...............................................................................................................14
    3.1.1 Statistics ............................................................................................................................15
    3.1.2 Big data ............................................................................................................................15
    3.1.3 Predictive Analytics ..........................................................................................................16
      3.1.3.1 Predictive Modelling .................................................................................................16
      3.1.3.2 Machine Learning .....................................................................................................17
    3.1.3.3 Data Mining ................................................................................................................18
  3.2 Dissecting a Profile ................................................................................................................18
  3.3 Gathering Data .......................................................................................................................19
    3.3.1 Gathering Data Directly from the Data Subject ...............................................................19
    3.3.2 Gathering Data from Cookies ..........................................................................................20
    3.3.3 Gathering Data from Settings .........................................................................................20
    3.3.4. Gathering Data from Purchases ....................................................................................21
  3.4 Uses of Data Profiling ...........................................................................................................21
    3.4.1 Dynamic pricing ................................................................................................................22
    3.4.2 Directed Marketing ...........................................................................................................23
    3.4.4 Credit scoring ....................................................................................................................23
  3.5 Problems with profiling .........................................................................................................24
    3.5.1 Faulty Processing/Errors ..................................................................................................24
    3.5.2 Collecting too Much Data ...............................................................................................25
    3.5. Normalization and Customization .....................................................................................25
    3.5.4 Dataveillance ....................................................................................................................26
4 Data Protection ....................................................................................................................27
  4.2 The GDPR and personal data processing .................................................................27
  4.3 Personal Data under the GDPR ...............................................................................28
  4.4 Data Protection Principles ........................................................................................29
    4.4.1 Lawfulness, Fairness and Transparency ...............................................................29
    4.4.2 Further Processing and Purpose limitation ..........................................................30
    4.4.3 Data Minimization ...............................................................................................31
    4.4.4 Accuracy ...............................................................................................................31
    4.4.5 Retention and Storage Limitation .......................................................................32
  4.5 Lawful Processing ......................................................................................................32
    4.5.1 Consent to Processing .........................................................................................33
    4.5.3 Processing Necessary for Compliance with a Legal Obligation ..........................34
    4.5.2 Balancing of interests ..........................................................................................35
  4.6 Automated Decision Making ....................................................................................35
    4.6.1 Automated Decision Making Including Profiling ...............................................36
      4.6.1.1 Decisions Based Solely on Automated Processing Including Profiling Which Produces Legal Effects or Similarly Significantly Effects ..........................................................37
      4.6.1.2 Legal Effect ...................................................................................................38
      4.6.1.3 Similarly Significant Effect ..........................................................................38
    4.6.2 Profiling and Direct Marketing under the GDPR .................................................39
      4.6.2.1 Targeted Advertising and Similarly Significantly Affect .................................40
    4.6.3 Exceptions from the General Prohibition in Article 22 Regarding Automated Decision Making Including Profiling ..........................................................40
      4.6.3.2 Profiling with Explicit Consent ....................................................................41
  4.7 Rights of the Data Subjects ........................................................................................42
    4.8 Separating the Personal Data from a Profile ..........................................................43
    4.8.1 The Article 29 Working Party on Personal Data ..................................................43
    4.8.2 The ECJ in YS – narrowing the definition of personal data? ..............................44
  5 Analysis: Personalized pricing and the GDPR ............................................................47
    5.1 Is the GDPR applicable? ..........................................................................................47
    5.2 Personalized Pricing and the Data Protection Principles ........................................48
      5.2.1 Personalized Pricing and Lawfulness, Fairness and Transparency ....................48
      5.2.2 Personalized Pricing and Further Processing and Purpose Limitation ..............49
      5.2.3 Personalized Pricing and Data Minimization ....................................................49
      5.2.4 Personalized Pricing and Accuracy ...................................................................49
      5.2.5 Personalized Pricing and Retention and Storage Limitation .............................50
    5.3 Personalized Pricing and Legal Grounds ...............................................................50
      5.3.1 Personalized Pricing and Consent .....................................................................50
      5.3.2 Personalized Pricing Balancing of Interests ......................................................51
1 Introduction

1.1 Background

The abundance of data coupled with technology has paved way for predicting future events and behaviors. When personal data is compiled to assess various characteristics, a profile is created. Profiles range from revealing personal interests to marital status and financial situations and health. Profiles may also reveal purchasing behavior and purchasing power. Analyzing a buyer’s behavior and customizing offers may be appreciated by users. A directed advertisement for hotels at discounted prices in Barcelona could be appreciated by someone who has recently searched for flights to Barcelona.

A price is personalized when it has been given to a certain person due to various factors pertaining to this person in question. The practice of assigning different prices to different buyers is nothing new. Haggling is a common practice in bazaars and agriculture markets in some countries. A merchant at a fruit stand may eye his or her potential customer and offer a price depending on how much he or she would think they could pay. With technology, it is however possible to collect data and map buyers who are not price sensitive and offer them goods or services at higher prices than others. This practice risks buyers paying more if their profile finds him or her to have a strong purchasing power.

---


The General Data Protection Regulation (GDPR)\(^5\) regulates data processing in general and profiling in particular. The definition of “personal data” poses the question of whether a profile should be regarded as “personal data” or not and how the GDPR is applicable to such processing. Given the lack of guidance and case law from the European Court of Justice (ECJ), it is not established how the “personal data” should be interpreted. The Data Protection Directive (DPD)\(^6\) regulates data processing and profiling but will be replaced by the GDPR. Some of the European Union’s (EU) and ECJ reasoning is therefore found in old case law and doctrine relating to the DPD. While the GDPR appears to broaden the definition of “personal data”, it is uncertain to what kind of profiling the regulation will be applicable and how its various articles and recitals should be interpreted. The possible intrusive effects of profiling and the dubiousness of the applicability of the GDPR therefore warrant further investigation.

Given seller’s access to large amounts of data and the technology to harness data, buyers risk being at a disadvantage due to having less information. This thesis therefore focuses on the relationship between commercial sellers who profile using personal data in order to personalize prices for buyers on the internet.

### 1.2 Aim and Research Question

This thesis sets out to discuss the legality of using personal data to create profiles which can be used for personalized pricing of items or service for commercial actors to buyers from a data protection perspective.

- How does the GDPR regulate personalized pricing on the internet between commercial actors and buyers?

---


1.3 Definitions
This thesis focuses on the relationship between commercial actors wishing to use data profiling technology to gather information about buyers. Various concepts and words will be described as they appear in the text. A few expressions are however vital for an understanding of the text and will be presented as they are defined in article 4 of the GDPR. "Personal data" refers to any information relating to a data subject. A "data subject" is an identified or identifiable natural person. Processing refers to the act of doing something with personal data, such as saving, structuring, collecting or deleting it. "Controller" is the natural or legal person who decides the purpose and is responsible for the processing. "Processor" is the natural or legal person which processes personal data on behalf of the controller.

1.4 Methods and material
By examining the relationship between the use of personalized pricing and the GDPR, this thesis will illuminate the problem from a perspective of legal informatics. This aims at illuminating how the law and information communication technology (ICT) interact with each other. By studying case law, directives, regulations and proposals from the EU, the thesis will contain a discussion of interpreting EU-law. Since the GDPR has not entered into force at the time of authoring, many parts of the interpretations and discussions will be hypothetical. For guidance, the preambles of the GDPR have been used when interpreting its articles. As support, the Article 29 Data Protection Working Party’s opinions (Article 29 Working Party) have been used when interpreting the EU’s stance on data protection. Some of the Article 29 Working Party’s opinions are from the DPD but most are from the GDPR. Due to the similarities of the DPD and the GDPR, the DPD will serve to illuminate the reasoning of the EU in questions of data protection.

10 The Article 29 Working Party is a working party created by the EU to independently advice and work for a uniform compliance of the data protection directive in the member states.
Addressing the intersection of the law and ICT, the thesis will discuss the phenomena of regulating personalized pricing through data protection law with the help of the methodology of proactive law. Seipel defines proactive law as jointly using legal and technical strategies to develop the information society according to specific blueprints and using it as a strategy for risk management. Using economic theory, the phenomena of price discrimination will be presented in order to understand the theory and functioning of personalized pricing. The technological foundation of data profiling will be presented to establish how technology has the ability to affect the economy. The GDPR will be presented as the way means for regulating the use of the technology. The GDPR will then be analyzed based on the presentation of the price discrimination in order to reach a discussion regarding the intersection of the economics of price discrimination, profiling technology and data protection law. This leads to using the tools provided by economics, technology and law, to reach a discussion of how regulating the processing of personal data in fact regulates personalized pricing and how and why it is necessary.

1.5 Delimitation

The thesis discusses personalized pricing by private sellers in order to maximize profit from the perspective of the GDPR. The potential use of profiling by state actors will therefore not be discussed. Personalized pricing is regulated by various areas of the law. Due to the practice being used by companies against individuals, consumer protection law is applicable. Given a discriminatory ground, personalized pricing may also be used to discriminate individuals and may therefore also be affected by discrimination law. Personalized pricing and big data could also be used to offset fair competition, which is why the practice has to comply with competition law. Given the complexity of personalized pricing, discussing its legality would require analyses of various areas of law. However, given the advent of the GDPR, its potentially high sanctions and its focus on protection data subjects, the focus of this thesis will be how the practices stand in relation to the GDPR.

12 Ibid p. 360.
1.6 Outline

Chapter two presents the economic theory behind price discrimination for an understanding of the phenomena and a market problem. In order to illustrate the interplay between economic theory and technology, chapter three follows by presenting the concept of profiling, including its various uses, risks and the technology. Chapter three also explains how data is gathered. In order to gain an understanding of how personalized pricing and profiling are regulated, chapter four presents data protection and the GDPR, including a deconstructed presentation of the various requirements of the GDPR. Given the complexity of the GDPR and personalized pricing, there are several aspects which have to be considered when profiling. These are discussed in chapter five in order to reach an insight as to under which circumstances profiling would be compliant with the GDPR. Chapter six features a discussion on whether personalized pricing actually poses a problem and how it is regulated under the GDPR, as well as some thoughts on how to regulate profiling differently. Finally chapter seven concisely concludes this thesis by hopefully clarifying the conclusions.

2 Price Discrimination

In economics, price discrimination describes the practice of selling the same services or goods at different prices to different buyers.13 The main reason for price discrimination is to tie the price to buyers’ demand and their willingness to pay, as opposed to tying the price to production costs.14 Using different price points for different buyers requires knowledge of those buyers and their ability to pay as well as of the market. This requires an estimate of the buyers’ inclination and possibility to pay for a product or a service.15 Price discrimination is generally divided into three tactics.16

2.1 Degrees of Discrimination

2.1.1 Third Degree Discrimination

“Third degree discrimination”, also known “group pricing”, refers to the activity of assigning a certain price to a certain group of people. The price can be decided by purchase histories, geographical locations, behavior patterns, age or whatever makes a group of people different. Typical situations for the use of group pricing is student discounts and senior citizen discounts. A common reason for group pricing is price sensitivity. Group pricing therefore uses general characteristics of groups of people to set prices specific prices for certain groups of people.

2.1.2 Second Degree Discrimination

“Second degree discrimination”, also known as “menu pricing” or “versioning”, refers to situations where sellers decide the price in relation to how the product is sold. The manner in which a product or service is sold may refer to tailored packages for buying in bulks or ticket prices changing depending on how much time there is before would have to be used.

2.1.2.1 Amazon’s Group Pricing

Amazon was one of the first actors on the internet whose dynamic pricing practices garnered attention. In September 2000, Amazon used various prices for the same DVD. A user was shown an initial price when he or she first visited the site, as a returning customer. However,

17 Ibid., p. 44.
18 Shapiro & Varian, pp. 44-45.
19 Shapiro & Varian, pp. 53-54.
20 Ibid.
21 Amazon is the largest internet retailer in the world. Even though Amazon is not stationed in Europe and the event took place before the advent of the GDPR, the scope of the GDPR extends to the processing of personal data of union members irrespective of the establishment of the controller or processor, article 3(2) GDPR. The event therefore not only serves as an example of the practice of dynamic pricing but as an example of a practice which will be affected by the GDPR.
after having deleted the cookies which categorized him as a returning customer, the DVD was offered at a lower price. Buyers who had bought DVDs had begun comparing prices of online retailers and noticed that Amazon’s prices for the same DVDs had varied between buyers. This was due to Amazon having conducted a pricing test, offering a 30%, 35% or 40% discount off the suggested retail price to DVD buyers. The buyers’ reactions ultimately lead to Amazon paying the difference to those who were offered the lower discount.

2.1.3 First degree discrimination

The last variation or price discrimination is “first degree discrimination” or “personalized pricing”. Personalized prices are prices which have been set for a certain person for a certain object or service. Computers analyze and categorize buyers’ behavior, resulting in systems with sales data, customer lists and price suggestions.

2.2 Information asymmetry

If one part knows more than the other, there is an information asymmetry. Akerlof coined the expression by shedding light on a common situation when dealing with used cars. When a person buys a used car, the seller will probably have had the car for a while and formed an opinion regarding the car. The buyer will however not be privy to all of the seller’s information. The buyer is left with analyzing the presented facts and whatever knowledge he or she has of the market and of cars in general. The buyer will therefore not be as informed

23 A cookie is a file which a browser saves which enables websites to recognize a visitor.


27 Shapiro & Varian, pp. 40-44.

28 Maggiolino, p. 7.


30 Ibid., pp. 488-491.
as the seller and will have to take a chance and hope that the seller is not withholding and information.\textsuperscript{31} Trust, therefore becomes one of the determining factors when making the decision to buy a used car. The buyer may not have sufficient information when deciding to purchase the car, but will rather have to trust the it is a good purchase.\textsuperscript{32}

3. Profiling

Profiling describes the practice of compiling personal data and evaluating and analyzing various aspects of that data.\textsuperscript{33} Hildebrandt states that the purpose of profiling is to select, and include and exclude objects or people.\textsuperscript{34} The GDPR defines profiling in article 4(4):

\begin{quote}
‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
\end{quote}

The definition found in the GDPR is similar to the lexical definition provided by the Oxford English dictionaries, which defines “profiling” as “the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people”.\textsuperscript{35}

Johnson defined profiling as “the activity of creating small but informative summaries of a database”.\textsuperscript{36} Data in profiles is not limited to “human data” and can also constitute data

\begin{itemize}
\item \textsuperscript{31} Ibid.
\item \textsuperscript{32} Ibid., p. 500.
\item \textsuperscript{33} Gutwirth & Hildebrandt, \textit{Some Caveats on Profiling}, in Gutwirth, Poulet & De Hert, \textit{Data Protection in a Profiled World}, pp. 31-32.
\end{itemize}
pertaining to animals, objects or relations between them. By classifying, describing and analyzing the summaries of data, a profile is created. Profiling enables predicting potential outcomes or probably expectations. This production of knowledge is known as knowledge discovery in databases (KDD). By comparing and analyzing data, the profiles reveal patterns and correlations. Comparing past occurrences on a large scale, offers probable predictions of the future.

Profiling can be used for various purposes. It can for example be possible to map a customer’s purchasing habits and then offer discounts or suggestions based on their previous shopping history. It is also possible to provide credit ratings through analyzing a person’s past transactions and debts.

### 3.1 How Profiling Works

A profile is the result of data combined with other data. Data profiling began using algorithms to assess the quality of data and statistical analysis of data values in a data set and exploring how value collections across data sets related to each other. Algorithms are named after the Persian mathematician al-Khwārizmī and defined by Brassard and Bratley as "[…] a set of rules for carrying out some calculation, either by hand or, more usually, on a machine". Given a set of data of various columns in a table, data profiling reveals a frequency distribution for the various values. The frequency distribution shows the number of times a variable takes each of its possible values and shows the number of occurrences of

---


38 Ibid.


42 Loshin, p. 94.

different values and allows understanding of the use of each column. The algorithm is then the dedicated process which is used to discover the patterns. Analyzing the findings, it is possible to find overlapping value sets showing new relationship between entities. This analysis may in turn reveal information which was not previously known.

3.1.1 Statistics

Given a set of statistics for a group of people it is possible to collect variables from this group and search for patterns. For example, a car dealer may keep track of his or her sales. The sale information coupled with the area code of buyers would on their own reveal which part of town each buyer lived in. By using an algorithm, it is possible to compare the cost of the car and the area code of its buyer. With the aid of the algorithm, it would be possible to establish that buyers from certain parts of town usually bought more expensive cars. The algorithm would then reveal that people from certain parts of town are less price sensitive than the rest of the town.

3.1.2 Big data

Lacking an official or legal definition, “big data” is used to describe data sets which are big enough to need supercomputers. A data set is special in the fact that it constitutes of data from multiple sources stored a single file. Databases on the other hand are a collection of

---

44 Loshin, p. 94.
45 Ibid.
data which may be found across various files.\textsuperscript{50} boyd and Crawford creatively describe “big data” as:

“a cultural, technological, and scholarly phenomenon that rests on the interplay of:

1. Technology: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets.
2. Analysis: drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims.
3. Mythology: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy.\textsuperscript{51}

3.1.3 Predictive Analytics

Big data is used for predictive analytics. Predictive analytics constitutes of various statistical techniques, such as predictive modelling, machine learning and data mining, which are used to analyze facts about the presents and the past to be able to predict future behaviors or events.\textsuperscript{52}

3.1.3.1 Predictive Modelling

Predictive modelling uses statistics to predict future events or behaviors. Finlay predictive models as:

“A predictive model captures the relationships between predictor data and behaviour, and is the output from the predictive analytics process. Once a model has been created, it can be used to make new predictions about people (or other entities) whose behaviour is unknown”.\textsuperscript{53}

\textsuperscript{50} Ibid.


\textsuperscript{53} Finlay, p. 215.
Greenstein describes predictive modelling as an intersection of statistics, mathematics, machine learning and artificial intelligence. A main component of predictive modelling is the mathematical algorithm which examines the data and searches for correlations and patterns. Predictive modelling may then be used to predict anything from weather conditions to human behavior.

3.1.3.2 Machine Learning

Machine learning is the phenomena of computers learning without being explicitly programmed. Machine learning explores the construction of algorithms used by computers, which in turn learn to predict future events or behaviors. Machine learning is useful when the creation of a certain algorithm, using sample inputs, would be impractical. Machine learning is for example often used for e-mail filtering and detection of data breach. Since unwanted e-mails often comes from different addresses, it is hard to create a universal algorithm sorting the unwanted e-mails. Machine learning is thus useful since a computer can learn from previous accounts of e-mail and learn from that information to be able to identify altered version of it. Detection of data breach works in the same way, that after a data breach has been rectified it would be in the interest of the one whose data were breached to safeguard themselves from similar new attacks. Attackers would then be forced to invent new ways to attack if computer systems keep learning how to protect themselves against new forms of data breach.

54 Greenstein, p. 23.


3.1.3.3 Data Mining

Given a large set of information but no way to harness it has been described as “a data rich but information poor situation”. If there is too much data to handle, the data loses some of its value since it will be difficult to extract any worthwhile information. The definition of data mining may be broad or more narrow. More narrowly, Han, Kamber and Pei define data mining as “an essential process where intelligent methods are applied to extract data patterns”. More broadly however they define data mining as “the process of discovering interesting patterns and knowledge from large amounts of data”. The data sources can include databases, data warehouses, the internet, other information repositories, or data that is streamed into the system dynamically. Data mining may be seen as methods which utilize the intersection of machine learning, statistics and database systems to extract valuable information from large amounts of data.

The sheer power of data mining enables new insights into problems and phenomena which could change the world for the better. Big data on the other hand also risks creating a big brother society with increased surveillance and private as well as public actors being able to predict data subjects moves.

3.2 Dissecting a Profile

There are various discussions of how to approach a set of data depending on whether it is possible to tie the data in the set to a person or not. Professionals working with these issues also carry various opinions on the topic. Clarke, as well as Roosendaal for example, separate

---

58 Han, Jiawei; Kamber, Micheline & Pei, Jian, Data Mining: Concepts and Techniques, 3rd ed., Morgan Kauffman, 2011, p. 5 [cit. Han, Kamber & Pei].

59 Ibid., p. 8.

60 Ibid.

61 Ibid.

62 Ibid.

63 Ibid.
“digital personae” from “profiles” when discussing data profiling. Clarke coined the expression “digital persona” and defines it as “a model of an individual’s public personality based on data and maintained by transactions, and intended for use as a proxy for the individual”. A key factor in Clarke’s definition is the representational aspect. The functioning as a proxy for a certain individual leads to the digital persona being limited to the data set that has an identifying connection to an individual. A distinguishing factor is however that the purpose of the digital persona and the data needed to create it are known before it is created. Rosendaal compares the creation of a profile to the filling out of a template, where the attributes are known beforehand.

3.3 Gathering Data

For a profile to exist, it needs to contain data. There are however various ways of acquiring data.

3.3.1 Gathering Data Directly from the Data Subject

The most obvious way of gathering data is through the data subject submitting it him- or herself. Collecting data directly from the data subject is common when users create profiles by entering personal information on websites. Personal information may also be required when carrying out purchases online or when joining loyalty clubs. Information may however also be gathered in more indirect ways. If a data subject fills out a form or query and enters personal data, it is possible that this information is stored in order to data subject.

---


66 Roosendaal in Becchi et. al., pp. 227-228.

67 Ibid.


69 Ibid.
3.3.2 Gathering Data from Cookies

Cookies are small pieces of data which websites can store on computers or mobile devices. Cookies allow websites to access users’ preferences and actions over time.\textsuperscript{70} Whenever the website which stored the cookies is visited by the same browser, the information found in the cookie will be read by the server. The server will then be able to remember the user’s browsing history for as long as the cookie is stored.\textsuperscript{71} While cookies are commonly used, most browsers have an option to reject cookies or to at least ask users to accept or reject them.\textsuperscript{72}

Cookies without an expiration date are called “session cookies” and remain saved for as long as the browser is open.\textsuperscript{73} Cookies which last longer are known as “persistent cookies” and last as long as their expiration date permits, after which they are deleted.\textsuperscript{74} Cookies thereby constitute an important source of information when profiling, by helping websites track and identify the behaviors of their visitors.

3.3.3 Gathering Data from Settings

While not as common as the other ways in which to gather data, it is possible to gather data by collecting a computer’s settings. To create an optimized display of a website, browsers transfer certain data when accessing them. This practice can reveal the version of the browser, operating system, which plug-ins are installed, headers, cookie settings, time zone and monitor resolution.\textsuperscript{75} By combining the data, it is possible to create a distinctive browser fingerprint. The browser fingerprint, in combination with other data information such as IP-

\textsuperscript{72} Ibid, p. 15.
\textsuperscript{73} Ibid.
\textsuperscript{74} Ibid.
\textsuperscript{75} Alich, Stefan & Voigt, Paul, Mittelesame Browser – Datenschutzrechtliche Bewertung des Trackings mittels Browser-Fingerprints, Computer und Recht, 2012, pp. 344-345.
addresses, allow websites to identify returning users who are not using cookies. The combination of data allows for a tracking and monitoring similar to that of cookies, even though the user may have actively rejected the usage of cookies.

3.3.4. Gathering Data from Purchases

It is possible to purchase personal data. The people selling personal data are known as data brokers. Personal data is usually sold in bundles at fairly low prices. The personal data market enables actors who might not be able to collect the data themselves to still acquire it. Actors may simply not have the means nor the demographic to collect it directly from the data subjects, and are then able to purchase the data. One of the main problems with data broking is however that it very often occurs without the knowledge of the data subjects. The data brokers are able to collect data from publicly available sources and compile, package and sell it. This practice creates a privacy risk for data subjects, as multiple brokers may sell data pertaining to a data subject without his or her knowledge.

3.4 Uses of Data Profiling

Data profiling may be used for different purposes and its prediction capabilities of monitoring human behavior are of big value to businesses and governments. It is also possible attempting to foresee future needs and use the information for product development. An

---

76 Ibid, pp. 344 & 346-347.
79 FTC, p. iv.
80 Ibid.
82 Germain, Richard, Were banks marketing themselves well from a segmentation perspective before the emergence of scientific inquiry on services marketing?, in Journal of Services Marketing vol. 14 issue 1, MCB UP Limited, Oklahoma, 2000, pp. 44-62.
actor may predict a need or a lack of a certain function or item and be able to act upon this with the help of the information gained by profiling.

3.4.1 Dynamic pricing

Dynamic pricing refers to the situation when a price is not fixed. This means that the price can change amongst other things depending on the time, across buyers or across products or a combination. The service is thereby adjusted depending on the current market demands. By using algorithms to determine the price, a business owner or the person setting the price is able to take competitor pricing, supply and demand and other external factors into mind when determining the price. Personalized pricing is therefore a form of dynamic pricing, seeing the prices vary depending on the person and the circumstances surrounding him or her.

Dynamic pricing is neither new in the hospitality industry. It is common for hotels to daily adjust their room rates depending on their occupancy. If the occupancy is low, the hotel is able to underprice a room but still lose less money than it would or break even, if the room had been continued empty. A common example of dynamic pricing is also Uber’s “surge pricing” which adapts the price of a car ride to the number of people ordering or trying to order a car at a certain time. What makes the use of profiling for dynamic pricing interesting is its reach – while adjusting a prices according to who the seller is talking to or the occupancy of a hotel, it becomes vastly different when it becomes as widespread as it does with the help of ICT. In this instances, ICT creates a great information asymmetry in favor of the seller. Buyers are able to compare prices, but will not know as much as sellers in regards


84 Rouse, Margaret, *What is dynamic pricing?*, TechTarget, 2015 (available at [http://whatis.techtarget.com/definition/dynamic-pricing](http://whatis.techtarget.com/definition/dynamic-pricing), accessed 1/1-2018.)


to previous and predicted behavior, and will therefore be at an information disadvantage in comparison with the sellers.

3.4.2 Directed Marketing
By adapting marketing strategies to different customers and creating personalized advertisement, it is possible for commercial actors to direct its marketing. With directed marketing, there is a bigger chance of positive reaction than with generic marketing. It is easier for a potential buyer to disregard something mundane but if it is something this person in particular can relate to, the advertisement has a higher chance of affecting the person.88 This actor thereby improves the revenue by foreseeing needs.

3.4.3 Monitoring employee behavior
Profiling may also be used for monitoring employee behavior to either detect fraud or to map and rank employees’ skills and productivity.89 Profiling is also used for forensic science. By mining patterns and seeing similarities between various cases, suspects and databases it is possible to combat crime and solve cases more effectively.90

3.4.4 Credit scoring
Through credit scoring, data profiling plays a role in the financial industry when assessing a possible borrower’s ability to repay a loan.91 Credit scores aim at representing a person’s creditworthiness by quantifying the risks associated with a borrower not being able to meet his or her credit obligations. By compiling and analyzing certain personal attributes, it is

---


possible to create a statistical set which represents a person’s creditworthiness. Profiling is also used in the financial industry to identify and prevent fraud and theft. Through pattern recognition software, it is possible to scour data for patterns which are characteristic for fraud and theft and develop mechanisms to prevent and more easily discover such behavior. Profiling also helps locate deviances from behavior in financial systems, which may not be connected to something illegal, could serve to bring out irregular behavior warranting a closer inspection.

3.5 Problems with profiling

When data is used to predict future events or behavior, profiling risks being intrusive. The data is there not a description of reality, but an analysis of probabilistic processing of data. More recently however, profiling is used more for describing a kind of predictive analytics. This means that computers may know more about a person this person knows of themselves. This data might then be used for purposes unknown for the data subject. The data subject then risks having this data used without his or her knowledge.

3.5.1 Faulty Processing/Errors

Errors made in the profiling process risk leading to incorrect decisions being made during automated decision making. Depending on the type of decision, the data subject might be affected unfairly. The GDPR has provisions to prevent such unfair processing, such as article 22 which is a general prohibition from automated decision making including profiling, unless certain requirements are met. Inaccurate data, either from a faulty profiling process or from wrong data from the start however risks having a negative impact on the data subject.

---


94 Ibid.

95 Greenstein, p. 40.
3.5.2 Collecting too Much Data

A main trait of big data that its main value is not necessarily connected to its primary purpose. This means that the main reasons for the personal data being collected will not correspond with its use with big data. The value of the data would therefore have to be calculated through all of the possible ways in which it could be used in the future. This risks personal data being used for other purposes than the data subject intending it to be. It has for example, been possible to predict private traits such as sexual orientation, ethnicity, religious and political views, age and gender from likes on Facebook.

3.5. Normalization and Customization

Growing accustomed to a service which uses data profiling carries various risks. Whether knowingly or unknowingly becoming used to receiving personalized information and offers, risks normalization of customization. A profile is created using somebody’s previous behavior and preferences. Information and offers are then personalized using the profile. The person being profiled will receive information and offers based on his or her profile. This person will in turn act upon that knowledge and information which has been directed towards him or her. This type of directed information risks affecting people. If a person is unaware of the fact that he or she is receiving one-sided information, he or she may believe the information to not be one-sided and act as if it were not. This person will have normalized the customization and therefore risk acting upon one-sided information. A person could then assume that the information he or she is being presented with is objective, when in fact it is personalized and determined according to a profile. When customization such as this occurs, it risks being normalized. If a person is unaware of the fact that the information he or she is receiving is directed, he or she may adapt his or her behavior to that information and start acting


97 Ibid., p. 107.

98 Kosinski, Michal; Stillwell, David & Graepel, Thore, Private traits and attributes are predictable from digital records of human behavior, Proceedings of the National Academy of Sciences of the United States of America, vol. 110 issue 15, 2013, pp. 5802-5805.

accordingly, not realizing that the information is influencing his or her behavior. Given that everybody is subjected to advertisements daily, receiving personalized advertisements risks catching people off guard and therefore poses a greater risk to a person’s privacy than general advertisements.

3.5.4 Dataveillance

A “Big Brother society” as envisioned by George Orwell in 1984 was seen as improbable when the book was released in 1948. With today’s technology however, data surveillance (dataveillance) is possible. Dataveillance is the continuous monitoring of communications and actions across various platforms. This could consist of the monitoring of the combined data from card transactions, social network usage as well as information available from public and private databases. Dataveillance combined with data mining creates a greater threat to privacy than human controlled surveillance. Solove argues that machines, unlike humans, are only interested in knowledge about the risks regarding our future behavior. Data would therefore not be collected for a specific purpose, it would rather be collected and analyzed for a possible future event, should it ever be needed. Surveillance controlled by humans is limited by the human and would therefore not be as intrusive as a machine collecting everything.

Solove holds that the information available from data mining and dataveillance is less like “Big Brother” and more like Kafka’s The Trial. Solove likens this with the protagonist of The Trial, who desperately tries to find out why he has been arrested but is sent through a bureaucracy labyrinth. Data mining creates a way for such a great amount of information to be extracted and stored, without a necessary purpose. Those whose data is stored are not

100 Hildebrandt in Hildebrandt & Gutwirth (eds.), Profiling the European Citizen pp. 307-308.
101 Clarke, The Digital Persona, p. 77.
104 Ibid.
105 Solove, p. 8.
always aware of what and how much of their data is stored and like Kafka’s protagonist, data subjects risk not being privy to what information there is about them or how it is being used.

4 Data Protection

“Data protection” is an umbrella expression for principles according to which data should be processed.106 These principles aim at balancing the conflicting values of privacy, free flow of information and governmental need for knowledge about persons for surveillance and taxation for example.107 The fundamental principles of data protection have been established by international organizations such as the Organisation for Economic Cooperation and Development (OECD), the Council of Europe and the EU. Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data are from 1980 from the OECD and Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data is from 1981 from the Council of Europe.

Personal data is protected by the European Convention of Human Rights in article 8 under the right to a privacy as well as article 8 of the EU Charter of Fundamental Rights. On an EU level, data protection is further regulated by the DPD and the national laws but will be replaced by the GDPR when it enters into force on May 25th 2018.

4.2 The GDPR and personal data processing

The GDPR is applicable if data processing occurs with a relation to the EU. Its scope is outlined in article 2 and 3 which state that the GDPR is applicable if the processing takes place in the context of the activities of an establishment of a controller or a processor in the EU. The GDPR is also applicable if the data subject is outside of the EU if the processing is related to the offering of goods or services or monitoring of behavior taking place in the EU.

106 Gutwirth & De Hert, in Hildebrandt & Gutwirth, Profiling the European Citizen, p. 281.

107 Ibid.
Activities falling outside the scope of EU law and purely personal or household activities by natural persons are exempted from its scope according to article 2(2) of the GDPR.

If the GDPR is applicable, the data has to be processed in accordance with the data protection principles in article 5. Lawful processing also requires a legal basis, which are found in article 6. The data protection principles are rather comprehensive but stipulate that the data should be processed lawfully and transparently and that it should only be collected for specific, explicit and legitimate purposes and be relevant and accurate. The legal bases range from consent from the person whose data is being processed to a contractual obligation or the legitimate interests of the controller or a third party.

4.3 Personal Data under the GDPR

The definition of personal data found in the GDPR is more comprehensive than the one found in the DPD and makes a special note of that online identifiers, such as IP addresses and cookies\textsuperscript{108} can constitute personal data.\textsuperscript{109} This reflects the change in technology and the manner in which information is collected.\textsuperscript{110} Even personal data which has been pseudonymized can be considered personal data under the GDPR depending on how hard it is to connect the pseudonym to a certain individual.\textsuperscript{111}

Article 2(a) DPD

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;


\textsuperscript{109} The Article 29 Data Protection Working Party considered cookies containing unique user ID:s to clearly be personal data in their opinion 1/2008 on data protection issues related to search engines.


\textsuperscript{111} Ibid.
Article 4(1) GDPR

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

4.4 Data Protection Principles

The data protection principles are found in article 5 of the GDPR and state that data should be processed lawfully and fairly and that as little data as possible should be processed and stored for as short of a period of time as possible. In the GDPR, this is referred to as lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

4.4.1 Lawfulness, Fairness and Transparency

Article 5(1)(a) of the GDPR requires data processing to be lawful, fair and transparent. Since profiles reveal correlations and have the ability to reveal information which earlier might not be known, it is often difficult for data subjects to comprehend that they in fact are being profiled and in which way.112 Article 12(1) of the GDPR requires the controller to provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data. Article 12(1) coupled with the requirement of lawful and transparent processing in article 5(1)(a) give the data subject a right to not only know that his or her personal is being used for profiling purposes but also how it is being used.

Fairness in data processing generally involves transparency.113 Part of the fairness assessment depends on how the data is obtained. If the data is obtained through deception or misleading,

---


113 Ibid.
the processing will be considered fair. For the data processing to be fair, the data should only be processed in ways which the data subject could reasonable expect and the data should not be used in ways which unjustifiably have a negative effect on the data subjects.

4.4.2 Further Processing and Purpose limitation

Article 5(1)(b) of the GDPR limits the purposes for which personal data should be processed. Profiling risks using personal data for other purposes than it was originally collected. Navigation software can often easily calculate where a person lives and works. The purpose of such data processing is for the user to easily be able to find his or her way home or work. By establishing where a person usually his or her days and nights, it is possible for to approximate a his or her home address and workplace. If such software uses the data to personalize advertisements, the further processing is not line with the purpose of the original processing. Whether the further processing is compatible with the original purposes of the data collection depends on the factors laid out in article 6(4) of the GDPR. These are, but are not limited to:

- any link between the original purposes of the data collection and the purposes of further processing
- the context in which the data has been collected, the expectations of the data subject and the consequences the data subjects may suffer due to further processing
- the nature of the data (in particular sensitive personal data)
- the existence of safeguards

The purpose limitation requires the purposes be specified, explicit and legitimate. The purposes cannot be too general or too vague. If a purpose is to “Improve user experience”, “marketing” or IT-security”, it will usually not be sufficiently explicit. The extent to which a purpose should be specified varies on the type of data and in which context it is collected.

---

114 Ibid.

115 Ibid.


117 Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, p. 52.
The Article 29 Working Party illustrates the purpose specification by comparing a small boutique to a large retail company.

The small boutique has a mailing list of 200 people to which it sends an annual catalogue to home addresses. When asking to receive the catalogue as well as in the catalogue itself, the subscriber is informed that it is possible to unsubscribe at any time, in person, by writing, by mail or by phone. The subscribers are also informed their data will only be used for the sending of the catalogue and will not be shared with other parties. According to the Article 29 Working Party this could be a sufficient purpose limitation.118

If the seller on the other hand were a large retail company, encompassing the entire European market, which uses profiling to send personalized offers and targeted advertisement, the purposes of the practice would have to specified in a more detailed way, as well as the decisional criteria for the profiling, describing on what grounds the decision was made.119

4.4.3 Data Minimization

Article 5(1)(c) of the GDPR requires data processing to be adequate, relevant and limited to what is necessary. When personal data is used for profiling, more data usually yields better results. This conflicts with the data minimization requirement. The provision requires data processing to be limited to what is necessary for the purpose for which it is processed.120 Data controllers should therefore be able to justify their need to collect and store their data. Since big data relies on heavy amounts of data, it is of importance to attempt to minimize the data processed in some way to be compliant with the data minimization requirement.

4.4.4 Accuracy

Article 5(1)(d) of the GDPR requires data to be accurate and up to date. This provision requires that controllers and processors have are aware of the accuracy of the data being processed. The large amounts of data lead to it being harder for data controllers and

118 Ibid.
119 Ibid.
120 GDPR Recital 39.
processors to be aware of how accurate the data being processed is. If certain people lack access to the internet or simply do not use the internet, they may be underrepresented when profiling. On the other hand, frequent users of the internet and social media risk being overrepresented. There is also a risk for data subjects to knowingly enter false data over the internet to be able to keep maintain a distance and privacy.\textsuperscript{121} The skewed representation risks creating a skewed and inaccurate result.\textsuperscript{122} Processing the inaccurate result would then not be compliant with the accuracy requirement of the GDPR.

4.4.5 Retention and Storage Limitation

Article 5(1)(e) of the GDPR requires data to be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”. “Kept in a form” refers to the way which data is stored and not the medium on which it is stored.\textsuperscript{123} It is for example importance whether the data is encrypted or divided and stored on different databases in order to prevent identification of the data subject.\textsuperscript{124} As stated in the provision, the data should permit identification of the data subjects.

If the profiles are dynamic, it is necessary to frequently review the information and ensure that it is accurate and still relevant to the purpose. The retention of data is dependent on its purpose. For profiling to be effective, much personal data is needed to be able to create as comprehensive a profile as possible. This would however risk conflicting with the requirement of storage limitation. Complying with the storage limitation would weaken the profile, making it less effective.

4.5 Lawful Processing

Article 6 of the GDPR requires a legal basis for data processing to be lawful. The legal basis for processing personal data and profiling has to be documented in order to comply with the

\textsuperscript{121} Article 29 Working Party on Automated decision making, p. 19.
\textsuperscript{122} Ibid.
\textsuperscript{124} Ibid.
accountability requirement found in article 5(2) of the GDPR. The accountability provision requires that controllers be responsible for demonstrating compliance with the principles of data processing. The legal bases found in article 6 of the GDPR are a) consent, b) necessity for the performance of a contract, c) necessary for compliance with a legal obligation, d) necessary to protect vital interests, e) necessary for the performance of a task carried out in the public interest or exercise of official authority, and f) necessity for the legitimate interests pursued by the controller or by a third party.

4.5.1 Consent to Processing

Article 6(1)(a) of the GDPR provides consent as a possible legal ground for data processing. Article 7 as well was Recitals 32-33 and 42-43 of the GDPR regulate consent. A consent should be freely given, specific, informed and unambiguous. Consent is required for each purpose of the processing. When using consent as a legal ground, controllers shall show that the data subjects are aware of exactly what they are consenting to as well as possible consequences.

For the consent to be free, the data subject should not feel forced to consent to data processing and there should be no negative consequences if the data subjects choose to not consent.¹²⁵ This aims at combating power imbalances between employees and employers and individuals and public authorities.¹²⁶ To guarantee the data subject transparency and user control, a consent should be specific, optional and informed for each purpose of the data processing.¹²⁷ For the consent to be informed, the data subject should to exactly what he or is consenting.¹²⁸ According to the Article 20 Working Party, this includes, but is not limited to: information about the controller and the purposes of the processing, they type of data will be processed,


¹²⁶ Article 29 Working Party on Consent, pp. 6-7 and Recital 43.

¹²⁷ Ibid. pp. 12-13 and Recital 43.

¹²⁸ Ibid. pp. 13-14 and Recital 42.
the possibility of withdrawing consent, potential profiling and potential third country transfers.  

4.5.2 Processing Necessary for Performance of a Contract

Article 6(1)(b) and the exception found in article 22(2)(a) state that data processing and decisions made solely by automated means including profiling may be lawful if they are necessary for entering into, or the performance of, a contract. The necessity of the decision is dependent on the contractual objectives of the two parties. This could depend on multiple factors such as greater consistency or fairness in the decision making process or improving the efficiency of the process. The threshold for something being considered a necessity is however high and there should it should be the least privacy intrusive method available.

4.5.3 Processing Necessary for Compliance with a Legal Obligation

Article 6(1)(c) gives a legal ground for data processing it necessary for a legal obligation. There should be a basis in law but it is not necessary for it to have been passed by parliament, Recital 41 and 45 of the GDPR. Due to a lack of guidelines regarding the interpretation of article 6(1)(c), the guidelines released by the Article 29 Working Party for the corresponding proviso in the DPD (article 7(c)), will be used. The data controller or processor does however have to be obliged to follow the law, a voluntary law is not sufficient for a legal ground. The law does however have to derive from the EU or a member state. Laws from other states, such as the Sarbanes-Oxley Act of 2002 from the United States, requiring whistleblowing schemes,

129 Ibid.


131 Article 29 Working Party on automated decision making, p. 12.

does not create a legal ground for processing under article 6(1)(c). Processing may be necessary for legal obligations where employers have to report salaries of employees or where financial institutions are required to report suspicious transactions under anti-money-laundering rules.

4.5.2 Balancing of interests

Article 6(1)(f) of the GDPR provides a general clause, allowing balancing of interests to result in a legal ground. The general clause grants a legal ground for data processing if the data processing is necessary for the purposes of the legitimate interests of the controller or a third party, unless those interests are outweighed by the fundamental rights and freedoms of the data subject. The legitimate interest however has to be in consideration to the processing in question and is interpreted in a broad manner. When balancing the interests, reasonable expectations of the data subject in relation to the controller have to be evaluated.

4.6 Automated Decision Making

Automated decision making refers to the “ability to make decisions by technological means without human involvement”. Automated decision making may or include profiling. Profiling is a varied concept and the Article 29 Working Party the use of profiling into three different concepts; general profiling, decision making based on profiling and solely automated decision making, including profiling. General profiling is simply the of profiles, while the other two concepts use profiles in the decision making process.

---

133 Article 29 Data Protection Working Party on the notion of legitimate interests of the data controller under Article 7 of the directive 05/46/EC, WP259, p. 19.

134 Ibid.

135 The general clause does however not apply to the processing carried out by public authorities in the performance of their tasks according to article 6(1) phrase 2 and Recital 47 of the GDPR.

136 Voigt & von dem Bussche, p. 103.

137 Ibid.

138 Recital 47 of the GDPR.

139 Article 29 Working Party on automated decision making, p. 7.

140 Ibid.
Automated decisions range from speeding fines solely imposed on the fact that a single camera has caught a vehicle speeding\textsuperscript{141} to for example the Swedish congestion taxes which are automatically taken out when a car passes a certain point at a certain time\textsuperscript{142}. These kinds of decisions, which are taken without any analyzing, are examples of automated decision making without profiling. If the decision to fine the driver instead were based on the driver’s driving habits over time such as if it is a repeated offence or if there are other traffic violations, it would be an automated decision making, including profiling\textsuperscript{143}.

\textbf{4.6.1 Automated Decision Making Including Profiling}

The definition of profiling found in article 4(1) of the GDPR\textsuperscript{144} implies that data processing which is not “automated” would not actualize the GDPR\textsuperscript{145}. Recital 24 suggests that profiling requires more than simply creating profiles. For example, the intention of taking decisions concerning a data subject or predicting a data subject’s behavior or preferences\textsuperscript{146}. That profiling would require a consequence is mentioned in Recitals 60 and 63, which stipulate the data subject’s right to be informed of the consequences of profiling.

The solely automated decision making including profiling is specifically regulated in article 22 of the GDPR. Article 22 is a general prohibition from the practice due to the higher risks associated for adverse effects that are associated with automated decision making including profiling\textsuperscript{147}. Exemplifying the concept of profiling, if a human bank worker decides to grant a

\begin{thebibliography}{9}

\bibitem{141} Ibid., p. 8.
\bibitem{143} Article 29 Working Party on automated decision making, 8.
\bibitem{144} As referenced in section 3 of this thesis.
\bibitem{146} Ibid.
\bibitem{147} Ibid.
\end{thebibliography}
loan to a client of a bank based purely on a profile generated through automated means, it is a decision based on profiling.\textsuperscript{148} If an algorithm on the other hand decides whether or not the person is granted a loan, it is a solely automated decision including profiling.\textsuperscript{149} The difference lies in the fact that the former decision ultimately was made by human while in the latter case the decision was ultimately made by a computer.

The way in which article 22 is written leaves room for interpretation whether data subjects have to exercise his or her right to not be subjected to automated decision-making, including profiling, or whether it is a statutory prohibition.\textsuperscript{150} For the provision to successfully protect individuals from decisions automatically taken by machines, it should be interpreted as a legal prohibition or at least a legal restriction on those kinds of processing activities.\textsuperscript{151}

\textbf{4.6.1.1 Decisions Based Solely on Automated Processing Including Profiling Which Produces Legal Effects or Similarly Significantly Effects}

If profiling is used for general purposes or if there is a human factor involved the general rules of the GDPR apply. If, however, there is a decision which is solely based on automated processing, including profiling, and the decision produces legal effects concerning the data subject or similarly significantly affects him or her, there is a general prohibition against such processing in article 22 of the GDPR.

If the decision is “based on solely automated processing”, there is no human involved in the decision making process. Therefore, if a person reviews automated decisions and has the power to change them, the decision is not solely based on automated processing.\textsuperscript{152} For human intervention to quality under article 22 if has to be meaningful and not merely a gesture. All

\textsuperscript{148} Ibid.
\textsuperscript{149} Ibid, and Recital 71.
\textsuperscript{150} Voigt & von dem Bussche, p. 180.
\textsuperscript{151} Ibid., and GDPR Recital 1 and 4.
\textsuperscript{152} Ibid p. 9.
data should be considered and the person reviewing should have the power to change the decision.  

The applicability of article 22 requires that a decision be taken by automated means without any human assessing the content of the decision. This means that the provision would be applicable when no human has decision-making powers, notwithstanding whether her or she is involved in the decision-making process, for example by scanning documents which could be relevant for the automated decision-making. This means that the provision is also applicable when a final verification of an automated decision is dependent on human verification, if the person is not able to influence the decision content.

4.6.1.2 Legal Effect

While legal effect is not defined in the GDPR, the WP29 interprets it as “a processing activity that has an impact on someone’s legal rights”. Legal rights range from the freedom to associate with others and voting in elections, to taking legal actions. Legal rights could also be something which affects somebody else’s legal status or contractual rights. WP29 exemplifies this by being entitled to or denied social benefits, being refused entry at the border, being subjected to increased security measures or being automatically disconnected from one’s phone service for forgetting to pay the bill.

4.6.1.3 Similarly Significant Effect

The general prohibition from using profiling for decision making by solely automated means prohibits the data processing if it has a legal effect. The article however extends this to

---

153 Ibid., p. 10.
154 Ibid., p. 181.
155 Ibid.
156 Ibid.
158 Ibid.
159 Ibid.
160 Ibid.
decisions “similarly affecting him or her”. Thus the GDPR compares a legal effect to an effect similarly affecting the data subject and therefore protects the data subject in this regard. Data subjects may then be protected from automated decision making, including profiling even if there is no legal effect.\footnote{\textsuperscript{161} Mendoza, Isak and Bygrave, Lee, The Right not to Subject to Automated Decisions Based on Profiling, University of Oslo Faculty of Law Legal Studies Research Paper Series no. 2017-20, p. 12.}

To similarly significantly affect the data subject means that the profiling has an effect which is equivalent or similarly significant in its impact.\footnote{\textsuperscript{162} Article 29 Data Protection Working Party on automated decision making, p. 10.} WP29 however holds “the threshold for significance must be similar, whether or not the decision has a legal effect”.\footnote{\textsuperscript{163} Ibid.} This means that for the effect to be considered significant it has to be of a certain, but still unknown, magnitude. The profiling must have the possibility of significantly influencing circumstances or behaviors.\footnote{\textsuperscript{164} Ibid.} Other examples found in Recital 71 of the GDPR include the “automatic refusal of an online credit application” and “e-recruiting practices without any human intervention”.\footnote{\textsuperscript{165} Ibid.} This broad interpretation of the provision makes it hard to determine how significant an effect must be to be covered by article 22. Recital 38 of the GDPR also holds that if an automated decision targets a child, the effect should be considered significant.

\subsection*{4.6.2 Profiling and Direct Marketing under the GDPR}

Processing personal data for direct marketing can be carried out for a legitimate interest according to recital 47. The data subject should, according to article 21(2) and Recital 70, however have the right to object to such processing, including profiling, alluding to the fact that direct marketing does not constitute profiling as such. Article 21 grants data subjects the right to object if profiling takes place with the public interest or legitimate interest as a legal...
basis. In the profiling related to direct marketing, the data subject has an absolute right to not be subjected to processing for such purposes according to article 21.3 of the GDPR.

4.6.2.1 Targeted Advertising and Similarly Significantly Affect

Discussing the meaning of “similarly significantly affect”, it is worthwhile comparing its meaning in the case of targeted advertising. If a fashion outlet decides to target all women in a certain region, the article 29 Working Party is of the opinion that the advertising would probably not have a significant effect. Depending on the certain characteristics of the case in question, it is however possible that it would. The article 29 Working Party found that the intrusiveness of the profiling has to be taken into consideration, the expectation and wishes as well as particular vulnerabilities of the individuals concerned as well as how the advertisement is delivered. Directed advertisement may therefore have various effects on various groups of people. Someone addicted to alcohol would be more susceptible to directed alcohol advertisement as opposed to somebody who is not addicted to alcohol. In the case of differential pricing, the effect could be significant if prohibitively high prices would in effect prohibit someone from certain purchasing certain goods or services. Worth noticing is that the effect can be positive as well as negative.

4.6.3 Exceptions from the General Prohibition in Article 22 Regarding Automated Decision Making Including Profiling

Article 22 imposes a general prohibition from decisions based solely on automated means. Article 22(2) however permits automated decisions being made if it is (a) necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.

167 Article 29 Working Party on automated decision making, p. 11.

168 Ibid.

169 Ibid.

170 Ibid.
In the case of an automated decision being made due to a contract or a data subject’s explicit consent, article 22(3) still requires the controller to allow the data subject to be able to contest the decision. For profiling as a necessity for a contractual obligation see chapter 4.5.2 of this thesis.

4.6.3.2 Profiling with Explicit Consent

The GDPR already requires a “clear affirmative act” for a consents in Recital 32. An explicit consent requires something more. The Article 29 Working Party has expressed that “explicit” refers to the way in which consent is expressed by the data subject.\textsuperscript{171} The working party suggests a written statement signed by the data subject, in order to secure an explicit consent but is also aware of the difficulties with such statements.\textsuperscript{172} An oral consent may be sufficiently explicit but would be hard to prove which is why some kind of documented statement is recommended.\textsuperscript{173}

There is no definition of explicit consent in the GDPR but according to the Article 29 Working Party, the consent should be “specifically confirmed by an express statement rather than some other affirmative action”.\textsuperscript{174} A consent may be withdrawn at any time according to article 7(3). It should be as easy for the data subject to withdraw his or her consent as giving it. Withdrawing consent does however not affect the lawfulness of any processing carried out during the time when there was a consent.

In a recommendation regarding profiling from the Committee of Ministers, it was submitted that as far as possible, and unless a service requires knowledge of a data subject’s identity, services should be available without having to communicate personal data.\textsuperscript{175} Striving for a

\textsuperscript{171} Article 29 Working Party on Consent, p. 18.

\textsuperscript{172} Ibid., pp. 18-19.

\textsuperscript{173} Ibid.

\textsuperscript{174} Article 29 Working Party on profiling, p. 13.

\textsuperscript{175} Council of Europe, Recommendation CM/REC (2010) 13 of the Committee of Ministers to member states. on the protection of individuals with regard to automatic processing of personal data in the context of profiling, p. 4.
specific, free and informed consent for the use of profiling, providers should have a default for non-profiled access to information about their services.\textsuperscript{176} To be able to use profiling without the data subject’s knowledge, the recommendation holds that it should only be allowed if it is expressly legal under domestic law as well as there being appropriate safeguards in place.\textsuperscript{177} Due to the lack of information regarding an explicit consent, it is hard to ascertain what where the line will be drawn between a regular consent and \textit{explicit} consent. The GDPR has high requirements for consent and as the Article 29 Working Party stated, an express statement rather than some affirmative action would make the consent more \textit{explicit}. It is however hard foretelling how express statements would practically function.

\textbf{4.7 Rights of the Data Subjects}

Due to the risk of profiling, articles 12(2)(f) and 14(2)(g) and 15(1)(h) grant the data subjects the right to be informed of this certain kind of data processing and its envisaged consequences.\textsuperscript{178} These rights force data controllers to not only inform the data subjects about profiling, but to also provide meaningful information about the logic involved as well as the potential consequences. The GDPR aims at protecting individuals in this case from being unknowingly profiled.

Requiring the information about the logic involved to be meaningful requires the controller to inform the data subject about the profiling in a sufficiently simple manner.\textsuperscript{179} The GDPR aims at protecting the data subjects by allowing them to make informed decisions. The requirement to provide the significance and envisaged consequences implies that information about future usage of the data must be disclosed as well.\textsuperscript{180} This requires actual situations which may

\begin{footnotes}
\item[176] Ibid.
\item[177] Ibid. and GDPR Recital 71.
\item[178] GDPR Recital 60.
\item[180] Ibid. and Council of Europe, \textit{Draft explanatory report on the modernized version of the CoE Convention 108}, 2016, section 75.
\end{footnotes}
occur. If a person knows how his or her data is processed, this person is more likely to make an informed decision. This levels the playing field when a person might not be aware of how his or her data is used for profiling or automated decision making.

4.8 Separating the Personal Data from a Profile

There are various discussions regarding whether a profile always constitutes personal data and if it is possible to separate the personal data from the profile. In 2008 Gutwirth and De Hert held that the traces of data used in profiling would activate data protection legislation. They were of the opinion that no profiling would be possible without personal data, because the data processed would in the beginning have been generated by the individuals. They reason that the fundamental data is necessary for the profiling to take place - consequently the data protection regulations should apply. There are however those who argue that an individual trigger is required for the data to be able to constitute personal data. Hildebrandt is for example of the opinion that the DPD is not applicable in many cases of profiling because it is uncertain whether the data used for profiling is *personal data*.

4.8.1 The Article 29 Working Party on Personal Data

The article 29 Working Party has held that something is personal data if it the information is “used to determine or influence the way in which that person is treated or evaluated”. The article 29 Working Party further holds that for data to be relatable to an individual there should be an element of “content”, “purpose” or “result”. The “content” then refers to information about a person, for example the results of a medical analysis relating to the

---

182 Gutwirth & De Hert in Hildebrandt & Gutwirth, *Profiling the European Citizen*, p. 288.
183 Ibid.
185 Hildebrandt in Hildebrandt & Gutwirth, *Profiling the European Citizen*, p. 322.
The “purpose” element refers to the element data being used with the “purpose to evaluate, treat in a certain way or influence the status or behavior of an individual.” The “purpose” instead focuses on the data impacting a certain person’s rights and interests in a specific case. The impact does not have to be big, it is enough if the data subject may be treated differently due to the data being processed. The Article 29 Working Party further holds that these three elements of data relating to an individual must be considered alternative and not cumulative. The Article 29 Working Party has therefore presented a wide definition of personal data.

4.8.2 The ECJ in YS – narrowing the definition of personal data?

In a ruling dealing with the definition of “personal data” under the DPD, the European Court of Justice (ECJ) left room for interpretation whether profiles always constitute personal data. In YS (C-141/12) v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel (C-372/12) v. M, S. (YS), the ECJ found that a legal analysis written by the Dutch immigration ministry, containing the ministry’s reasons and justifications when deciding on an applicant’s possibility of receiving a residency permit, was not personal data. The analyses generally contained the name, date of birth, nationality, gender, ethnicity, religion and language of the applicant. When requested, the applicants used to receive the legal analysis in its entirety. Due to the great workload of the ministry and common misinterpretation by the applicants, the Dutch immigration offices stopped handing out the analyses in their entirety. Instead they decided to release “a summary of the personal data.”

---

188 Ibid.
189 Ibid.
190 Ibid, p. 11.
191 Ibid.
192 Joined cases YS (C141/12) v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel (C372/12) v. M, S.
193 Ibid. section 14.
data contained in the document, including information relating to the origin of those data and, where relevant, the bodies to which they were disclosed.”.194

When deciding on the case, the ECJ found that a *legal analysis* containing typical personal data found in profiles, was not personal data.195 The court confirmed that the data regarding persons used to write the legal analysis was personal data.196 According to the court, the analysis on its own, is “in so far as it is not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant’s situation, that situation being established inter alia by means of the personal data relating to him which that authority has available to it”.197 While this information would still have a “purpose” and a “result”, which are recognized by the article 29 Working Party as characteristics of personal data, the ECJ ruled that the analyses did not constitute personal data.198 The article 29 Working Party has expressed that data with the purpose to “evaluate, treat in a certain way or influence the status or behavior of an individual” is typically personal data, thereby differing from the ECJ in YS.199

Korff holds that the reasoning of the court is wrong and that it undermines the purpose that the EU set out for data protection and narrows the definition of personal data.200 Consequently, the ruling limits the right of access to personal data as well as the functioning of the DPD.201 Korff compares the Article 29 Working Party’s Opinion on the concept of

---

194 Ibid., sections 16-17.
195 Ibid. sections 33-48.
196 Ibid. 38.
197 Ibid. section 40.
198 Article 29 Working Party on Personal Data, p. 10.
201 Ibid.
Personal data\textsuperscript{202} and extracts four defining elements for personal data.\textsuperscript{203} These are “any information”, “relating to”, identified or identifiable” and “natural person”.

Korff disagrees the most with the way the court treats the notion that personal data has to “relate to”, as stated in the definitions of the DPD and GDPR, an individual.\textsuperscript{204} Korff holds that information may relate to different individuals at the same time. Data could for example relate to one individual because of its content (it is about that person), to a second person because of its purpose (it will be used to treat person number two in a certain way) and to a third person because of its result (the impact the processing will have on the rights and interests of person three).\textsuperscript{205} Data would therefore not have to focus on a certain individual to relate to him or her. Korff argues that the notion that personal data has to relate to an individual limits the data subjects’ rights to challenge the accuracy of profiles, if profiles are too abstract to analyze, as the ECJ found in YS.\textsuperscript{206}

Lynskey on the other hand disagrees with Korff. In regards to profiles, Lynskey argues that “the judgment prevents individuals from accessing the logic underpinning a particular decision (therefore the algorithm generating the profile), but the information used to reach the decision as well as the decision itself (the outcome of the algorithm) may still constitute personal data”.\textsuperscript{207} Regarding predictive modelling and the YS case, Greenstein is of the opinion that for any meaningful insight into the process, access to the underlying logic of a decision is crucial.\textsuperscript{208} According to Greenstein, access to the data as well as the algorithm used when the decision was made are both necessary for satisfactory insight.\textsuperscript{209}

\textsuperscript{202} Article 29 Working Party on Personal Data, p. 10.

\textsuperscript{203} Korff.

\textsuperscript{204} Ibid.

\textsuperscript{205} Ibid.

\textsuperscript{206} Korff.

\textsuperscript{207} Lynskey, p. 123.

\textsuperscript{208} Greenstein, p. 335.

\textsuperscript{209} Ibid.
5 Analysis: Personalized pricing and the GDPR

The GDPR regulates profiling and personalized pricing. The applicability of the GDPR as well as actors’ compliance with it is however discussable. This requires an analysis of the way in which personal pricing takes place, how it complies with the general provisions of the GDPR, focusing on the data protection principles and legal grounds, as well as how it complies with article 22 dealing with profiling.

5.1 Is the GDPR applicable?

In light of the YS Case\textsuperscript{210} from the ECJ where the court found that the legal analyses were not to be considered personal data, raises the question whether or not profiles used for personal pricing would even constitute personal data.

While there is a lack of case law regarding data profiling, there may be similarities between legal analyses and profiles. The ECJ states that personal data constitutes personal data whether in a profile or not.\textsuperscript{211} However it is not as clear whether a profile on its own - without the information relating to a natural person – would still constitute personal data. The ECJ ruling is from the time of the DPD, which has a narrower definition of personal data than the GDPR. Oftentimes profiles are used in conjunction with their respective personal data but it is still uncertain if they are not and how the GDPR should be applicable to that kind of processing.

The characteristics of a legal analyses have similarities to a profile created for personalized pricing. The legal analyses contain arguments, reasoning and analyses on law regarding a certain person. This analyses were then used to make a decision. Profiles used for personalized pricing on the other hand constitute of personal data such as name, gender, purchasing history and approximated income, creating a profile estimating the maximum a person would pay for a product, used to make an automated decision on which price a particular person should be given.

\textsuperscript{210} Joined cases YS (C141/12) v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel (C372/12) v. M, S.

\textsuperscript{211} Ibid. section 38.
This leaves from for the question on whether a profile used for personalized pricing would stop being a profile if the original data on which is was created were removed. The definition of personal data in the GDPR is broader than the one found in the DPD. Theoretically, the ECJ watered down the concept of personal data with the ruling in YS but it is unclear to what extent the court will uphold this precedent after the GDPR comes into force. Using the reasoning found in the YS case, removing the personal data and solely keeping the arguments arguably exclude the profiles from the definition of personal data under the GDPR. In practice, separating the personal data from the profile would be hard if the profile were to be used for personalized pricing. The creation and use of profiles for personalized pricing are dependent on the profiles’ link to the data which the personalized price is aimed at. This makes circumventing the GDPR and detaching the personal data from the profiles unfeasible for personalized pricing.

5.2 Personalized Pricing and the Data Protection Principles

For data processing to be lawful, it has to be carried out in accordance with the data protection principles. The data protection principles are found in article 5 of the GDPR and are referred to as lawfulness, fairness and transparency; purpose limitation; data minimization accuracy; storage limitation; integrity and confidentiality and accountability.

5.2.1 Personalized Pricing and Lawfulness, Fairness and Transparency

In the case of personalized pricing, this means that the data subject would have to be informed of the fact that his or her data were to be used for profiling purposes which would lead to customized pricing. It also means that the data subject should be aware of the fact that the information he or she provides could be used for profiling and personalized pricing. Since the personal data is used for the profiling, the profiling and personalized pricing should not unjustifiably have a negative effect on the data subject. While uncertain, this gives rise to belief that the pricing ranges should not be too wide for the pricing to not have too much of a negative effect on the data subject.
5.2.2 Personalized Pricing and Further Processing and Purpose Limitation

If using profiling for personalized pricing, the purpose of the data collecting should therefore reveal that the personal data in fact will be used for personalized pricing. Stretching the purpose to include personalized pricing would depend on the way personalized pricing is used. As laid out in article 6(4) of the GDPR, further processing which is not encompassed by the original purpose may be permitted. If the original purpose were to send *customized advertisements* and the data subject were aware of this – *customized pricing* would not be within the original purpose but could still be close to the original purpose. The same kind of information may be used for both purposes and if the data subject were duly informed of the profiling taking place for the advertisement, he or she would be aware of the fact that the customized advertisement derived from stored personal data.

A data subject would in this case *expect* customized advertising but might be shocked to receive customized pricing if that purpose has not been made clear. If the effects of the customized pricing are positive but unexpected, the pros for the data subject would have to be outweigh the cons and the privacy intrusion. It is therefore theoretically possible for personalized pricing to use profiling for personalized pricing and not mention it in the purpose but it would be hard to justify.

5.2.3 Personalized Pricing and Data Minimization

The requirement for data minimization risks posing problems for profiling. Since profiling has the power to *create* new data, the new data might not be in accordance with the original purpose, which limits the new data from being lawfully processed according to the principle of data minimization. The legality is therefore dependent on the purpose and the exceptions to personal data being lawfully processed for another purpose, found in article 6(4) of the GDPR. The more data there is, the more accurate the profile becomes. Effective personalized pricing would therefore inherently clash with the principle of data minimization.

5.2.4 Personalized Pricing and Accuracy

The requirement of accuracy creates obligation for data profiling. Controllers will need measures and safeguards to ensure that the data used for profiling is accurate and up to
This supports the importance of providing clear information to the data subject so he or she is able to correct possible inaccuracies and improve the quality of the data. While applying to all kinds of data processing, it is hard to determine which effect this requirement would have on personalized pricing.

5.2.5 Personalized Pricing and Retention and Storage Limitation
Considering the fact that more data makes a profile more accurate, the storage limitation works limits the possibility of saving personal data for profiling. Complying with said limitations therefore makes the use of the profiles less effective and the prices set less accurate.

5.3 Personalized Pricing and Legal Grounds
Data processing requires a legal ground to be lawful, article 6 of the GDPR. Since personalized pricing is very much optional, it will not be necessary for the performance of a contract nor for the compliance with a legal obligation or to protect vital interests and probably not necessary for the performance of a task carried out in the public interest. These legal grounds will therefore not be discussed. The most relevant legal ground for personalized pricing is consent. A balancing of interests might be possible but will be hard to justify.

5.3.1 Personalized Pricing and Consent
It has been established that the requirements for a valid consent are high. For a person to consent to personalized pricing the consent would have to be freely given, specific, informed and unambiguous. The data subject would then have to be aware of which personal data that is being processed and freely give their consent to have their prices set using the personal data acquired by the seller as a basis for this price setting. The potential problem with today’s market is that it is questionable whether how many buyers are aware of sellers’ various price setting regimes. Consenting to going from general prices to personalized prices would therefore require much knowledge from the buyers and high standards for a lawful consent.

---


213 Ibid.
Practically speaking, a person may consent to personalized pricing if he or she believes that it would save money. Consenting to a dynamic price setting where a person risks paying more would not be common but could a possibility if the person thought the pros would outweigh the cons and that he or she would make money in the long run.

5.3.2 Personalized Pricing Balancing of Interests

A balancing of interests as a legal ground for personalized pricing would require the interest of the actor wishing to profile the buyer outweighing the buyer’s right to privacy as well as the buyer reasonably expecting it. A common interest of the seller would be to maximize revenue and sales. The buyer would reasonably expect that the seller would want to maximize his or her revenue and sales. The buyer’s privacy would however be disproportionately violated compared to what the seller has to gain.

A hypothetical scenario of a seller personalizing prices in order to automatically subsidize products or services to help buyers who would not be able to afford them would be discussable. The profiling is still however a great intrusion of privacy and would therefore be difficult justifying if only the data subjects receiving the subsidies have something to gain. The intrusion of privacy would simply be too great for those who will still be profiled but not receive any benefits.

5.4 Personalized Pricing under Article 22

While data processing for profiling has to live up to the requirements set out in the GDPR regarding data processing in general214, for the protection of article 22(1) to be activated there has to be a decision based solely on automatic processing including profiling which produces legal effects for the data subject or similarly affects him or her. Since personalized prices are automatically set using algorithms to harness sets of personal data, the practice would live up to the first requirement of the provision.

214 Recital 72.
5.4.1 Personalized Pricing Having a Legal Effect

When profiling is used for personalized pricing, a product may be offered at a customized price which could be higher or lower than the market price. If the data subject and data processor (or data controller) enter into a contract, the pricing will have led to a legal effect. The contract is however not a direct effect of the data processing; therefore, the processing has not produced a legal effect for the data subject. The question at hand is therefore if personalized pricing similarly significantly affects a data subject.

5.4.2 Personalized Pricing and Similarly Significantly Affect

While not identical, it is possible to compare personalized pricing and directed advertisement. Determining whether profiling used for personalized pricing has a similarly significant effect on the data subject therefore varies greatly depending on the situation. A profile could reveal a person has a smaller budget. This could then lead to that person being offered items at prices lower than market prices, to stimulate his or her purchasing habits and develop the business relationship. If prices of certain items were raised after having stimulated purchasing and a built a relationship, the practice would be intrusive, something the individual did not expect and due to trust being built, the individual would be vulnerable. Determining whether or not something has a similarly significant effect would therefore be dependent on the profiling and pricing in question. This could possibly have similarly significant effect.

5.4.3 Personalized Pricing and the Exceptions in Article 22(2)

If the requirements in article 22(1) are met there are exceptions found in article 22(2) of the GDPR. Article 22(2) allows the automated decision making including profiling it a) is necessary for a contract, b) is authorized by EU law or c) there is an explicit consent from the data subject.

If the personalized pricing has a legal or similarly significant effect, it would be difficult to justify under the exemptions in article 22(2). For it to be necessary for the performance of a contract, the use of profiling for personalized pricing would have to make the decision making process (the personalized price setting in this case) more fair or consistent.215 While having positive effects, it is not necessary to personalize pricing to sell items over the internet. It is submitted that the profiling is used to maximize profits for the sellers and there does not

---

make the decision process more fair or consistent. If the purpose of the profiling however were to level the purchasing power of low-income families, it would be possible to argue that it would make the decision making process more fair or consistent.

Personalized pricing is neither authorized by Union or Member State law. According to Recital 71, the purpose could be to monitor and prevent fraud and tax-evasion or to ensure the security and reliability of a service provided by the controller. Since personalized pricing is a way for a company to improve sales it would not qualify under this exception either. It would be possible to gather an explicit consent. The lack for clear guidelines regarding explicit consent makes the consideration on whether it can be possible harder. The requirements for a “normal” consent is already set high with the GDPR. Adding the word “explicit” therefore suggests there is even a higher requirement for it to be allowed. Considering the nature of the automated decision making and the information asymmetry associated with it, it would be natural for the data subject to be even more aware of the risks associated with the process.

6 Reflections

6.1 Does Personalized Pricing Pose a Problem?

Data profiling enables the harnessing of data on a massive scale. For a successful personalized pricing scheme information on a large scale is necessary. The combination of data profiling and personalized pricing therefore risks creating an information asymmetry for buyers. While buyers often are in a worse standing than sellers, this information asymmetry is more apparent. Since buyers risk not being aware of them being profiled, it creates a problem.

A general dynamic pricing regime applying to all buyers differs in the sense that everybody is treated equally. The widespread use has allowed people to get used to the fact that prices do change and it is not a surprise that a flight may be cheaper if bought two months in advance as opposed to a day before departure. Personalized pricing is however not as eminent, it is harder to notice and harder to make an informed decision. Given the informational requirements set out in the GDPR, where the data subject has to be informed of the practice and the rationale behind it, many people would not take their time and get sufficiently informed, leading to these people trusting the system.
This leads to the question if there is a real damage involved – if the prices are set in accordance with the maximum people want to pay and if people find the products or services to be worth it. Even though a person might pay a higher price for a certain product or service, it might not have too great of a negative impact on their economy. The price difference is however based on an information asymmetry. When prices are changed for everybody, everybody is affected the same way and it is easier to keep track of and understand. The intricacies of data profiling and personalized pricing are arguably however not easy for the common person to understand. If buyers mapped all of their personalized prices and compared them, this information asymmetry could be cured. There are price comparison websites available which help buyers combat the information asymmetry.

The problem is however that the vendors in this scenario have much greater power than their respective customers. Unless a data subject requests the personal data processed, he or she will not know how much data the data controller is processing. This risks leading to the seller painting of picture of the items sold at market price, questioning who would constantly be suspicious of pricing and the shoppers believing they are being offered goods and services to a market price.

6.2 Protection against Profiling
The GDPR protects data subjects by requiring that data be processed in accordance with the data protection principles, the requirement for a legal ground, the rights of the data subject as well as the specific regulation for automated decision-making including profiling. In general, it is difficult to be compliant with the strict requirements of the GDPR. The special requirements in article 22 for automated decision making including profiling requires even more of the data controller and processor. As discussed earlier, it is however possible to use profiling for personalized pricing in compliance with the GDPR.

The only legal ground for automated decision making including profiling for personalized pricing is consent. Acquiring a consent when a user registers for a website is not difficult. Ensuring the consent is compliant with the GDPR requires it to be freely given, specific,
informed and unambiguous. If the personalized pricing is deemed as having a *similarly significant effect* (to a legal effect), the consent would have to be *explicit*. Given the strict requirements for a consent and the information requirements, acquiring a consent which meets the standard of the GDPR might prove difficult.

Buyers would naturally be interested in ways of saving money, or at least not being overcharged. This requires sellers to sell themselves, to be able to attract the buyers. If buyers were aware of the fact that their personal data would be used to personalize their prices in order to maximize revenue and sales for the seller, the buyers consent is debatable. This creates a conflict between the sellers wish to maximize revenue and sales, as well as appeal to the buyers’ while still being honest about their data processing.

It is submitted that, if complied with, the GDPR will protect buyers from harmful personalized pricing tactics given the requirements for processing data. The practical issue is whether the GDPR will be complied with or not. In contrast to the DPD, the GDPR has strict sanctions which data controllers as well as data processors will wish to avoid. The interest for data protection has grown and unfair profiling would risk negative publicity. Uncertain of the economic effect of Amazon’s dynamic pricing in 2000\(^\text{216}\), the practice created bad publicity which is still remembered years later. The strict sanctions of the GDPR coupled with the potential bad publicity as a result of unlawful data processing, data controllers as well as processors have a stronger incentive to comply with the GDPR than they did the DPD.

### 6.3 Regulating Profiling Differently

It is possible to regulate the processing of personal data in various ways. Koops critizises the GDPR for trying too hard to regulate the *processing of data* as opposed to regulating the *protection of the individual*.\(^\text{217}\) Koops argues that the problem with analyzing cookies, profiles and Big Data is that it is possible to jointly analyze fragments of data and extract

---

\(^{216}\) As discussed in section 2.1.2.1.

disproportionate amounts of information. Koops therefore suggests a *sui generis* protection, meaning that there would not be a certain distinction between “personal data” and “non-personal data” but instead a prohibition from processing data which would have a certain effect on an individual. To provide examples, Koops mentions separate legal instruments for regulation profiling or mass surveillance and having data portability being protected in consumer protection law. Koops also suggests governmental data processing not being regulated through a data protection law but through public procedure law, by limiting the collection of personal data for governments. Koops also argues that article 8 of the ECHR might lead to lengthy and rigorous litigations but in the end prove to be a better way to combat unfair data processing by governments rather than relying on regular data protection laws and DPA regulation.

7 Conclusions

It is submitted that personalized pricing strategies risk negatively affecting buyers by subjecting them to an information asymmetry as well as a violation of privacy. The GDPR regulates the processing of personal data in general as well as profiling in particular. It is possible to use personal data for profiling and comply with the GDPR. If the GDPR is complied with the data subjects should receive sufficient information to not be severely harmed by the information asymmetry as well as being able to decide whether or not the profiling is worth the invasion of privacy. The remaining question is whether actors will comply with the GDPR or not.

---

219 Ibid.
220 Ibid.
221 Ibid.
8 Bibliography

8.1 Literature


Darbellay, Aline, Regulating Rating, Schulthess Verlag, Zürich, 2011.

Finlay, Steven, Predictive Analytics, Data Mining, and Big Data: Myths, Misconceptions and Methods, 1st. ed., Palgrave Macmillan, United Kingdom, 2014 [cit. Finlay].

Greenstein, Stanley, Our Humanity Exposed, Department of Law, Stockholm University, Stockholm, 2017 [cit. Greenstein].


Han, Jiawei; Kamber, Micheline & Pei, Jian, Data Mining: Concepts and Techniques, 3rd ed., Morgan Kauffman, 2011, [cit. Han, Kamber & Pei].


Roosendaal, Arnold, *Digital personae and profiles in law: Protecting individuals’ rights in online contexts*, Wolf Legal Publishers, Oisterwijk, 201


### 8.2 Articles and Journals


Mendoza, Isak and Bygrave, Lee, The Right not to Subject to Automated Decisions Based on Profiling, University of Oslo Faculty of Law Legal Studies Research Paper Series no. 2017-20, p. 12.


8.3 European Union

8.2.1 Regulations


8.2.2 Directives


8.2.3 Court of Justice of the European Union

Joined cases YS (C141/12) v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel (C372/12) v. M, S.

8.2.4 Article 29 Data Protection Working Party


Article 29 Data Protection Working Party on the notion of legitimate interests of the data controller under Article 7 of the directive 05/46/EC, WP259, 2014.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation. for the purposes of Regulation 2016/679.,
Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines.


Miscellaneous

Commission, com (92) 422 final – syn 287, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.


8.3 Council of Europe

Council of Europe, Recommendation CM/REC (2010) 13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.


8.4 Electronic Sources


