PART III
Contexts and Images of Digital Vulnerable Subjects

The Digital Vulnerability of Insurance Consumers and Personalised Pricing of Insurance Products*

Piotr Tereszkiewicz, Katarzyna Południak-Gierz, Patryk Walczak

A. Introduction

Modern technologies enable traders to personalise (individualise) contracts they conclude with consumers. Big data analytics has made it technically possible and commercially attractive to create profiles for individual consumers and provide them with personalised offers. The personalisation of content presented to online users has thus become a highly relevant legal issue. One is tempted to start by defining the notion of 'personalisation' itself.[1] Usually, personalisation is understood to mean the process of adjusting the online content presented to individuals depending on the data available on their situation, traits, and preferences.[2] The definition of personalisation may yet depend on whose perspective is assumed to describe it. From the perspective of the consumer, different methods of matching the content with the user may qualify as personalisation. These methods may all lead the consumer to believe that online content was tailored individually for them. If we understand personalisation in this manner, then it only occasionally entails *actual individualisation*: the content may be adjusted not to an individual user, but to the context in which the information is presented (e.g., context advertising) or to the typical characteristics of a targeted group (segment) of the population. Understood in this manner, personalisation is an umbrella term encompassing practices during which not only an individual but also a group of individuals can be the addressee (target), in particular, practices such as online contextual, segmented, and

* This Chapter has been written within the framework of a research project supported by the National Science Centre (NCN) in Poland, grant number 2018/29/B/HS5/01281.

1 We rely here on an excerpt from: Katarzyna Południak-Gierz and Piotr Tereszkiewicz, 'Digitalization's Big Promise and Peril: Personalization of Insurance Contracts and its Legal Consequences' in Klaus Mathis and Avishalom Tor (eds.), Law and Economics of the Digital Transformation, (Springer 2023) 34.

2 Eliza Mik, 'The erosion of autonomy in online consumer transactions' (2016) Law, Innovation and Technology 8, 19.

behavioural advertising.[3] Nevertheless, to define personalisation one can also assume a perspective which places technology at the centre. From this perspective, personalisation can be understood as a practice that involves using data collected from an individual's activity (e.g., purchase history, email activity, website behaviour) in order to deliver targeted content to that individual. Under this second approach, the terms 'individualisation' and 'personalisation' can be used interchangeably to describe the process in which the content is individually shaped for every addressee separately, based on their profile.[4]

Personalisation of contracts may, *inter alia*,[5] include personalisation of prices offered to individual consumers: typically, 'personalised pricing' oc-

3 Niklas Fourberg, Serpil Taş, Lukas Wiewiorra, Ilsa Godlovitch, Alexander De Streel, Herve Jacquemin, Jordan Hil, Madalina Nunu, Camille Bourguigon, Florian Jacques, Michele Ledger and Michael Lognoul, *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice*, Publication for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg 2021, 30-31; Christopher Townley, Eric Morrison and Karen Yeung, 'Big data and personalised price discrimination in EU competition law' (2017) 36 Yearb Eur Law, 689-690.

4 See Florent Thouvenin, Fabienne Suter, Damiane George and Rolf H. Weber, Big Data in the Insurance Industry: Leeway and Limits for Individualising Insurance Contracts' (2019) 10 JIPITEC, 210; Joanna Strycharz, Guda van Noort, Natali Helberger and Edith Smit, 'Contrasting perspectives – practitioner's viewpoint on personalised marketing communication' (2019) 54 European Journal of Marketing, 641; Marta Infantino, 'Big data analytics, insurtech and consumer contracts: a European appraisal' (2022) 30 Eur Rev Priv Law, 613; Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax and Joanna Strycharz, *EU consumer protection 2.0, structural asymmetries in digital consumer markets* (2021) <https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf>, 102; Południak-Gierz and Tereszkiewicz (n 1), 34. Personalisation mechanisms frequently rely on predictive analytics using big data sets – information fuelling the personalisation process is not only derived from the data on this person but also from other data sets on 'similar consumers' and statistical data, Mik (n 2), 20. The better the latter proxies are, the less information is needed about the actual preferences of an individual. Consequently, it can be argued that during the process of tailoring the information the point of reference is not a particular individual. The benchmark is the 'alter ego' of that individual, their digital representation construed within the digital environment, mostly for commercial purposes. This creates a problem which can be referred to as de-personalisation by personalisation tools, see Helberger, Lynskey, Micklitz, Rott, Sax and Strycharz (n 4), 103-104; Infantino (n 4).

5 In insurance (as well as in other instances where a specific risk is one of the crucial factors determining the values exchanged under a contract) personalisation of contracts may also take place solely with respect to provisions specifying insured

curs when traders use the data that they have collected to infer consumers' willingness to pay.[6] Even though the empirical evidence might be inconclusive, economic research suggests that personalised pricing, including price discrimination, does occur in practice.[7] In an extreme scenario, firms can set individual prices and fully extract consumers' willingness to pay to their economic advantage. In practice, traders usually employ indirect methods of personalised pricing, such as personalised discounts[8] or search discrimination.[9] Yet, as consumers end up paying different, personalised

risks, without extending to the personalisation of price because 'an insurance provider might have an interest in providing coverage (and therefore to engage in terms personalization) for additional events without raising the premium, as long as it does not increase its actual risk. (…) term personalization can play a major role in selecting how to include superabundant coverage and, at the same time, exclude relevant risks,' Antonio Davola, Fabrizio Esposito and Mateusz Grochowski, 'Price Personalization vs. Contract Terms Personalization' in Fabrizio Esposito and Mateusz Grochowski (eds), Cambridge Handbook on Price Personalization and the Law (Cambridge University Press, forthcoming).

6 Marc Bourreau and Alexandre de Streel, *The regulation of personalised pricing in the digital era* (OECD 2020) <https://one.oecd.org/document/DAF/COMP/WD(2018)150/en/pdf>, 2: 'We refer to both individual pricing and group pricing with small targeted groups as personalised pricing or price targeting'. Maurits Kaptein and Petri Parvinen 'Advancing E-Commerce Personalization: Process Framework and Case Study' (2015) 19 International Journal of Electronic Commerce, 9; Joost Poort and Frederik Zuiderveen Borgesius, 'Does everyone have a price? Understanding people's attitude towards online and offline price discrimination' (2019) 8 Internet Policy Review, 1.

7 Bourreau and de Streel (n 6), 3; Cristina Poncibò, 'The UCTD 30 Years Later: Identifying and Blacklisting Unfair Terms in Digital Markets' (2023) 19 European Review of Contract Law, 336.

8 Personalised discounts are very difficult to compare, which reduces the probability of consumers' negative reactions. Lan Xia, Kent B. Monroe and Jennifer L. Cox, 'The price is unfair! A conceptual framework of price fairness perceptions' (2004) 68 Journal of Marketing, claim that consumers may perceive personalised pricing as unfair, in particular when they observe they are paying a higher price for a similar product than other consumers. See also Kelly Haws and William Bearden, 'Dynamic Pricing and Consumer Fairness Perceptions' (2006) 33 Journal of Consumer Research, 304: price discrimination will often be regarded as unfair if it exceeds a certain level; Simon Lee, Abdou Illia and Assion Lawson-Body, 'Perceived price fairness of dynamic pricing' (2011) 111 Industrial Management & Data Systems, 531. For a different view Edwards (2006), 559.

9 Search discrimination or steering consists of showing different products to consumers from different groups, based on the available information about consumers, Bourreau and de Streel (n 6), 3.

net prices in such cases, those pricing strategies are equivalent to personalised pricing.[10]

Insurance is certainly one of business sectors in which the use of big data analytics has influenced the marketing and distribution stage in the value chain, enabling the rise of personalised insurance policies.[11] From a legal perspective, these developments merit close attention as technology based marketing and distribution strategies fall within the scope of EU consumer protection and data protection frameworks to which this Chapter will turn below.

B. Digital distribution of insurance and personalisation of insurance contracts

In the insurance sector, there are two most important criteria for the personalisation (individualisation) of insurance contracts.[12] First, personalisation is typically based on the risk profile of the consumer. In practice, insurers do not calculate the risk for each consumer but create groups of customers and offer premiums corresponding to the risk assessment for respective groups.[13] Insurance premiums reflect the assessments concerning the risk to be insured against.[14] Second, personalisation may be undertaken based on the consumer's willingness to pay (price optimisation).[15] Insurance regulators describe price optimisation as an insurer's use of sophisticated data mining tools and modelling techniques during the ratemaking

10 Bourreau and de Streel (n 6), 3.

11 Antonella Cappiello, *Technology and the Insurance Industry. Re-configuring the Competitive Landscape* (Palgrave Macmillan 2018); Bernardo Nicoletti, *Insurance 4.0. Benefits and Challenges of Digital Transformation* (Palgrave Macmillan 2021).

12 In this Chapter, 'personalisation' and 'individualisation' will be treated as synonyms. Thouvenin, Suter, George and Weber (n 4), 210, use the term 'individualisation' of insurance contracts with respect both to the consumer's willingness to pay and the consumer's risk profile.

13 Thouvenin, Suter, George and Weber (n 4), 211, indicating that this serves two important policy goals: the reduction of adverse selection and the avoidance of moral hazard.

14 Casualty Actuarial Society, *Generalised Linear Models for Insurance Ratings* (2nd edn, CAS Monograph Series No. 5 2020), available at https://www.casact.org/sites/default/files/2021-01/05-Goldburd-Khare-Tevet.pdf.

15 Thouvenin, Suter, George and Weber (n 4), 242; Barış Soyer, 'Use of Big Data Analytics and Sensor Technology in Consumer Insurance Context: Legal and Practical Challenges' (2022) 81 Cambridge Law Journal.

process to vary rates based on factors other than a person's risk of loss.[16] This means that insurers use non-causal risk proxies (e.g., shopping habits or internet searches) to determine whether a potential consumer is willing to pay more for the same product as opposed to others who are in the same risk profile.[17] Personalisation based on the consumer's willingness to pay results from the fact that consumers with a uniform or similar risk profile may have different needs for insurance cover, and perhaps more importantly, different financial resources for buying insurance products.

Undoubtedly, these two main criteria for personalising insurance contracts may be combined in practice when calculating the individual premium of a customer.[18] One must bear in mind that technological solutions used in the insurance industry automatically collect personal data about consumers, thus automatically performing a risk analysis according to a pre-defined algorithm, which in the end entails determining the price for the risk assumption by the insurer.[19] During this process, different types of data relevant for targeting a consumer are gathered and analysed.[20] What is crucial is that these data may be used not only for narrow actuarial purposes, i.e., calculating a premium, but also to increase the profit that an insurance distributor derives from a transaction. For instance, marketing techniques can be oriented towards artificially increasing consumers' willingness to pay, so that they opt for more expensive insurance products[21] or differentiating the price for different policyholders interested in purchasing the same insurance product.[22]

16 The Research Report, 'The Use of Price Optimization in Insurance Ratemaking', the Connecticut General Assembly <https://www.cga.ct.gov/2015/rpt/2015-R-0251.htm>.

17 Soyer (n 15), 183.

18 Thouvenin, Suter, George and Weber (n 4), 242.

19 Mário Čertický, 'Certain Issues of Innovations Affecting the Insurance Business in the in the Light of the GDPR and Hungarian Insurance Law' (2021) 10 Acta Universitatis Sapientiae Legal Studies, 51.

20 As to categories of personal data used for personalisation (individualisation) see Thouvenin, Suter, George and Weber (n 4), 210-211; Čertický (n 19), 38; Helberger, Lynskey, Micklitz, Rott, Sax and Strycharz (n 4), 103–104; Soyer (n 15), 169-170.

21 Peter Rott, Joanna Strycharz and Frank Alleweldt, *Personalised Pricing* (Publication for the Committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, 2022), 8; Oren Bar-Gill, 'Algorithmic Price Discrimination: When Demand Is a Function of Both Preferences and (Mis)perceptions' (2019) 86 University of Chicago Law Review, 218.

22 Piotr Tereszkiewicz and Katarzyna Południak-Gierz 'Liability for Incorrect Client Personalization in the Distribution of Consumer Insurance' (2021) 9 Risks, 84; for

There is no general principle of insurance law that forbids personalising (individualising) insurance prices (premiums).[23] It is worthwhile to emphasise that in the European Union, the requirement of prior approval of standard terms was abolished as a result of the deregulation of the insurance sector in 1992.[24] As a result of this revolutionary development, the internal market directives, both in life and non-life insurance, have introduced the formal prohibition of prior approval or systematic notification of general and special policy conditions, scales of premiums, or forms and documents which an insurance undertaking intends to use.[25] Article 181(1) of the Solvency II Directive provides that Member States shall not require the prior approval or systematic notification of general and special policy conditions, scales of premiums, or forms and other printed documents which an insurance undertaking intends to use in its dealings with policyholders. Under Article 181(2) Solvency II, Member States which make insurance compulsory may require that insurance undertakings communicate to their supervisory authority the general and special conditions of such insurance before circulating them.

By contrast, there might be specific provisions in different fields of law, possibly relating to different branches of insurance.[26] In this respect, U.S. law provides an interesting example. In the U.S. the insurance business is primarily regulated at a state level.[27] Most state insurance laws in the U.S. provide that 'insurance must be fair, available, and affordable'. Insurance rates are subject to statutory requirements: insurance rates cannot be excessive, inadequate, or unfairly discriminatory. Further, in most states

examples of such practices using data exploration see Zarsky, '"Mine Your Own Business!": Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion' (2003) 5 Yale Journal of Law and Technology, 19-21.

23 For an in-depth survey of Swiss and California legal systems Thouvenin, Suter, George and Weber (n 4), 242; see also Soyer (n 15).

24 Herman Cousy, 'Insurance law between business law and consumer law. Belgian report' in Eric Dirix and Yves-Henri Leleu (eds), *The Belgian Reports at the Congress of Washington of the International Academy of Comparative Law* (Brulyant 2011), 549.

25 Idem.

26 Thouvenin, Suter, George and Weber (n 4) provide a comparative overview of the laws applicable to the individualisation of insurance contracts in Switzerland and California/US.

27 See Tom Baker, Kyle D. Logue and Carolyn V. Williams, *Insurance Law and Policy: Cases and Materials* (Wolters Kluwer 2021), 613. Federal regulation does not play a significant role in governing the insurance business except for some federal statutes on health insurance.

property and casualty insurance rates have to be approved by state commissioners prior to use by insurers. Statutory protection against arbitrary insurance rates can be extended to prohibit personalised pricing as has become the case in the California insurance regulation: personalisation (individualisation) based on the consumer's willingness to pay in property and casualty insurance is straightforwardly excluded by way of a notice issued by the Insurance Commissioner in February 2015.[28] The Commissioner's Notice defines price optimisation as 'any method of taking into account an individual's or class's willingness to pay a higher premium relative to other individuals or classes'. The Notice states that price optimisation does not seek to arrive at an actuarially sound estimate of the risk of loss and other future costs of a risk transfer. In the Commissioner's view, any use of price optimisation in the ratemaking or pricing process is unfairly discriminatory and violates California law. It follows that under California insurance law there is no leeway for the personalisation of insurance contracts based on the consumer's willingness to pay. Importantly, several other state jurisdictions in the U.S. have followed California in barring the use of price optimisation in the ratemaking process.[29]

In what follows, we analyse market practices that involve the personalisation of insurance contracts in the light of GDPR and UCPD.[30] The question of the personalisation of insurance contracts appears particularly relevant as far as the interplay between those two regulatory regimes is concerned. Since data collection processes are essential in the insurance business and the use of personalisation tools is increasing in this sector,[31] there is always a possibility that personalisation tools might be applied in violation of GDPR to maximise the traders' profits. Should this happen, a trader's conduct

28 <https://www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/upload/PriceOptimization.pdf>. See Thouvenin, Suter, George and Weber (n 4), 218.

29 For a brief description see the Research Report 'The Use of Price Optimization in Insurance Ratemaking', the Connecticut General Assembly <https://www.cga.ct.gov/2015/rpt/2015-R-0251.htm>.

30 The analysis of the personalisation of insurance contracts under anti-discrimination law remains outside the scope of this Chapter; see Thouvenin, Suter, George and Weber (n 4), 220-227.

31 Thouvenin, Suter, George and Weber (n 4), 227; Piotr Tereszkiewicz, 'Digitalisation of Insurance Contract Law: Preliminary Thoughts with Special Regard to Insurer's Duty to Advise' in Pierpaolo Marano and Kyriaki Noussia (eds) *InsurTech: A Legal and Regulatory View. AIDA Europe Research Series on Insurance Law and Regulation*, vol 1. (Springer 2021), 127; Soyer (n 15), 166-167.

would certainly fall within the scope of UCPD as a potentially unfair commercial practice.

It must be stressed that the data analysed and processed for the individualisation (personalisation) of insurance contracts are typically the consumer's personal data hence they raise questions concerning privacy and data protection law; in the light of Article 4(1) GDPR, all the information relating to the data subject is personal data.[32] As far as sensitive data is concerned, the processing of genetic, biometric and health data of the data subject may typically arise in the context of insurance relationships.[33]

C. Personal data processing under GDPR

Under the General Data Protection Regulation (subsequently referred to as GDPR)[34] every processing of personal data[35] must have a lawful basis, such as consent of the data subject or a legitimate interest of the controller. Moreover, the processing must be carried out in accordance with the applicable data protection principles, which GPRD lays down as follows.

First, the data minimisation principle requires that the collection of personal data should be limited to what is necessary for the purposes for which they are processed (Article 5(1)(c)). Second, under the GDPR's accuracy principle, personal data must be accurate and kept up to date (Article 5(1)d). Data controllers are responsible for ensuring the accuracy of the data they compile about consumers, even if the data has been obtained from other sources. Third, the storage limitation principle of GDPR obligates data controllers to limit the storage of personal data to the timeframe necessary for their processing (Article 5(1)(e)). Fourth, the integrity and confidentiality principle requires data controllers to implement appropriate technical and organisational measures to ensure the security of personal data (Article 5(1)(f)). Finally, Article 20 of GDPR grants consumers a right to data portability, which allows them as data subjects to obtain from

32 Thouvenin, Suter, George and Weber (n 4), 227; Bourreau and de Streel (n 6), 6; Čertický (n 19), 38.

33 Čertický (n 19), 40, points out that such processing may arise in connection with fixed-sum insurance, specifically life and accident insurance as well as liability insurance.

34 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1.

35 Under Article 4(1) GDPR any information relating to an identified or identifiable natural person ('data subject') is considered personal data.

data controllers the personal data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

Typical examples of GDPR breaches by a trader may include: i) processing personal data without a proper legal basis; ii) processing special categories of personal data based solely on Article 9 GDPR, and without the explicit consent of the data subject; iii) using automated decision-making without any legal basis; and iv) failing to comply with information duties imposed by the GDPR. While these conduct types are discussed in the legal literature,[36] an assessment of whether the personalisation of insurance premiums is carried out in compliance with the GDPR may still pose a significant challenge in practice. Three major difficulties arise. First, one should note that the legal basis for processing personal data by an insurance distributor may differ depending on, among other factors, the relevance of data for a risk assessment by an insurance distributor.[37] Second, data processing within the insurance sector is highly automated, and therefore it needs to be verified as to whether automated data processing – a stage preliminary to decision-making – falls within the scope of Article 22(1) GDPR, and if so, whether it is covered by the exception provided for in Article 22(2) GDPR (see below). Third, verifying whether the process that leads to the personalisation of insurance premiums is sufficiently transparent may also be problematic.

I. Lawfulness of data processing under GDPR

From the perspective of the insurance business, personal data of consumers is necessary for both a risk assessment and the offering of adequate insurance products by insurance distributors.[38] Under the GDPR, the legal

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

37 Viktoria Chatzara, 'The Interplay Between the GDPR and the IDD' in Pierpaolo Marano and Kyriaki Noussia (eds) Insurance Distribution Directive (Springer 2021), 281.

38 On using processing data to prepare an offer see Ulrich Damman and Spiros Simitis, *EG-Datenschutzrichtlinie: Kommentar* (Nomos 1997), 149; Chatzara (n 38), 281.

basis for processing that personal data may be the 'processing necessity':[39] under Article 6(1)(b) GDPR, 'Processing shall be lawful if (…) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract.' 'Necessity' means that the purpose of the processing could not be fulfilled with anonymous information.[40]

The concept of 'processing necessity' is based on the conclusive consent of the data subject, i.e., the consumer.[41] The necessity of personal data processing requires investigating whether there are less intrusive means of assuring the appropriate performance of a contract, especially if the contract could be performed without the processing of personal data.[42] If that is the case, the necessity criterion under the GDPR is not fulfilled.[43] Further, Article 6(1)(b) GDPR stipulates that data processing may be lawful if it is necessary 'in order to take steps at the request of the data subject prior to entering into a contract'. This could be the processing of personal data in order to prepare an offer.[44] Following the same rationale, data processing is usually necessary to supply an offer of an insurance product to the consumer. Thus, it can be argued that the provision of Article 6(1)(b) GDPR can be considered the most suitable ground for processing personal data that are relevant for risk assessment as the latter is crucial for preparing an offer. It follows that, in so far as the personal data that is processed serves to determine the risks that are to be insured and affects the risk pricing, the processing of such data might be viewed as lawful under Article 6(1)(b) *in fine* GDPR.[45] Consequently, insurance distributors

39 Waltraut Kotschy, 'Commentary to Article 6' in Kuner, Bygrave, Docksey and Drechsler (n 36), 331; Čertický (n 20), 45-46.

40 Judgment of the Court (Grand Chamber) of 16 December 2008, Heinz Huber v Bundesrepublik Deutschland, Case C-524/06, ECLI:EU:C:2008:724, para. 62 ff.

41 Kotschy (n 39), 331.

42 Kotschy (n 39), 331; Thouvenin, Suter, George and Weber (n 4), 232. In its 2/2019 Guidelines, the European Data Protection Board stated that only objectively necessary processing operations may be based on this legal ground; the contract cannot 'artificially expand' the categories of personal data or processing operations beyond the data subject's reasonable expectations, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* (EDPB 2019), 8.

43 EDPB (n 42), 7.

44 Kotschy (n 39), 331.

45 It is submitted that the arguments raised in the analysis of whether this ground for processing can be invoked concerning price discrimination are not applicable in this context, see Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price

must carefully determine the personal data they need, to proceed with an accurate risk analysis, and collect from the consumer the data that is appropriate, adequate and necessary for such purposes in line with the data minimisation principle.[46] With respect to price personalisation based on the consumer's willingness to pay, it is submitted that the criterion of 'necessity' under GDPR may not be fulfilled. For the insurer can always rely on risk groups and is not obligated to personalise insurance contracts.[47] It follows that insurance distributors should rely on other grounds for the lawfulness of processing in cases involving the personalisation of insurance contracts, i.e., the consent of the consumer.

Further, one should emphasise that insurance distributors are obliged to explore the needs and wishes of clients and provide adequate explanations and advice.[48] These obligations result from the Insurance Distribution Directive[49] and national provisions on insurance contract law.[50] With respect to personal data that must be processed to comply with the above-mentioned obligations – i.e., data required to establish what insurance cover a consumer needs or wishes to obtain, the legal basis for processing shall be found in Article 6(1)(c) GDPR. Although Article 6(1)(c) GDPR does not usually justify data processing for marketing purposes in e-commerce,[51] it might provide a legal basis for data processing by insurance distributors: Specifically where the data is used to match the scope of products to be offered to consumers to meet their needs.[52] However, Article 6(1)(c) GDPR does not allow an insurance distributor to process that data for the purposes of the personalisation of the insurance premium as neither of

Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy, 360.

46 Chatzara (n 37), 282; Thouvenin, Suter, George and Weber (n 4), 230.

47 Thouvenin, Suter, George and Weber (n 4), 232.

48 Piotr Tereszkiewicz, *Obowiązki informacyjne w umowach o usługi finansowe* (Wolters Kluwer Polska 2015), 297-299; Tereszkiewicz (n 32), 142; Chatzara (n 38), 282.

49 Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution [2016] OJ L 26/19.

50 See Południak-Gierz and Tereszkiewicz (n 1), 42-44.

51 Katarzyna Południak-Gierz, Consequences of the use of personalization algorithms in shaping an offer – a private law perspective' (2019) 13 Masaryk University Journal of Law and Technology 2, 176.

52 Guidelines on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021), Official 2021/C 526/01, 18; On when such an obligation arises in the context of e-commerce see Tereszkiewicz and Południak-Gierz (n 22).

the abovementioned insurance distributor's obligations requires them to personalise insurance contracts based on the consumer's willingness to pay.

Finally, some personal data are processed by insurance distributors not because they are essential for risk assessment at the pre-contractual stage or because of the need to comply with the legal obligations of insurance distributors, but just for marketing purposes. In such cases, it could either be argued that processing is necessary for the purposes of the legitimate interests pursued by the controller (Article 6(1)(f) GDPR) or that the lawfulness of such personal data processing will depend on whether the data subject has consented to the processing of their personal data for these specific purposes (Article 6(1)(a) GDPR).

Further, under Article 6(1)(f) GDPR data processing is lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data. It could be argued that an insurance distributor has a legitimate interest in processing personal data for the assessment of insurance risk and the calculation of insurance rates. As long as the data taken into account is relevant from the perspective of risk assessment, it is reasonable to assume that, in principle, the controller has a legitimate interest in their processing and that interest is not overridden by the interests or fundamental rights and freedoms of the data subject. This might change once other data is analysed during the process of underwriting, especially if non-risk-relevant personal data is referred to and consequently, the premium calculated based on risk-relevant factors increases to match the insurance consumer's willingness to pay. Here, even if one were to conclude that there are no better-suited and less intrusive ways of safeguarding insurance distributor's interests (which is, however, unlikely), one might be inclined towards a view that the interests of the consumer and especially the right to privacy should override the aforementioned economic interests of the insurance distributor.[53] At the very least,

53 Agnieszka Jabłonowska, Francesca Lagioia and Giovanni Sartor in Fabrizio Esposito and Mateusz Grochowski (eds), Cambridge Handbook on Price Personalization and the Law (Cambridge University Press, forthcoming) argue that generally in the case of price personalisation, the consumer's interests outweigh those of the controller except for instances where personalisation cannot negatively affect the consumers' economic interest, e.g., consists solely in offering individualised discounts. Similarly Fabrizio Esposito, 'The GDPR Enshrines the Right to the Impersonal Price' (2022) 45 Computer Law & Security Review, 7, 12.

an approach based on the balancing of conflicting interests requires a case-specific assessment; a universal interest analysis is impossible.[54]

As for the consumer's consent to having their personal data processed, consent should be freely given, without any pressure;[55] otherwise, it will not be valid.[56] Further, the data subject ought to be informed about the specific purpose of data processing in a way that enables that data subject to understand the intended result of data processing. The main difficulty in this regard lies in the assessment of whether the aforementioned purpose was communicated in a sufficiently clear and precise manner. The technical jargon of insurance law makes it difficult for consumers to understand why their personal data is processed.

What is more, one should emphasise that one and the same piece of data could be used for more than one purpose. If these purposes are not compatible with one another, then an appropriate legal basis for the processing is required for each of these purposes.[57]

Finally, one should take into account the scope of data processed by an insurance distributor as it may cover data that fall within special categories of personal data provided for in Article 9(1) GDPR.[58] Consequently, the lawfulness of processing that data depends on whether, in addition to being covered by one of the situations listed in Article 9(2) GDPR, the requirements of Article 6 GDPR are met in a given case.[59] With respect

54 Thouvenin, Suter, George and Weber (n 4), 234.

55 Kotschy (n 39), 330.

56 Article 29 Data Protection Working Party Opinion (2011) 15/2011 on the definition of consent, 13.

57 Cécile de Terwange, 'Commentary to Article 5' in Kuner, Bygrave, Docksey and Drechsler (n 36), 315-316; Article 29 Data Protection Working Party 'Opinion (2013) 03/2013 on Purpose Limitation, 40; Thouvenin, Suter, George and Weber (n 4), 232. Soyer (n 15), 176, emphasises practical difficulties for insurers in complying with that requirement and recommends imposing specific restrictions on insurance companies' capacity to repurpose data. See also Paul MacDonnell, 'The European Union's Proposed Equality and Data Protection Rules: An Existential Problem for Insurers' (2015) 35 Economic Affairs, 233, observing that insurers using data mining techniques do not know what they will find until it is too late.

58 Jeffrey Amankwah and Nele Stroobants, 'GDPR and the Processing of Health Data in Insurance Contracts: Opening a Can of Worms?' in Margarida Lima Rego and Birgit Kuschke (eds) *Insurance and Human Rights. AIDA Europe Research Series on Insurance Law and Regulation,* vol *5.* (Springer 2022), 179.

59 Ludmila Georgieva and Christopher Kuner, 'Commentary to Article 9' in Kuner, Bygrave, Docksey and Drechsler (n 36), 376.

to this category of personal data,[60] one should point out that if such data is disclosed at the pre-contractual stage, explicit consent for its processing should be obtained. This requires a high standard of determining the purpose of processing and a precise wording of the respective consent[61] under Article 9(2)(a) GDPR) even if the requirement of processing necessity is fulfilled, as may be the case under Article 6(1)(b) GDPR and there is room for an implied consent. So as long as sensitive data is processed by an insurance distributor, explicit consent from the data subject is required; implied consent is not sufficient.

II. GDPR and automated individual decision-making

When it comes to fully automated individual decision-making that produces legal effects concerning the data subject or similarly significantly affects that data subject,[62] explicit consent to the processing of personal data is required under Article 22(2)(c) GDPR.[63] Personalising insurance prices could be an example of automated individual decision-making: Within this process, the algorithm decides on the price for a specific consumer, in a fully automated manner, and this affects the legal situation of the consumer as the process determines the extent of their contractual obligations should a contract be concluded.[64] Similarly, data processing based on Internet of Things (IoT) systems is regarded as automated decision-making, including profiling.[65] This suggests that where insurance distributors want to use automated processing for this purpose, even though the data processing it-

60 With the exception of employment and social security law.

61 Georgieva and Kuner (n 59), 377; Amankwah and Stroobants (n 58), 195; Soyer (n 15), 174.

62 On the nature of profiling and automated decision-making see Aleksandra Drożdż, *Protection of Natural Persons with Regard to Automated Individual Decision-Making in the GDPR* (Wolters Kluwer 2019), 10–16.

63 Lee A Bygrave, 'Commentary to Article 22 GDPR' in Kuner, Bygrave, Docksey and Drechsler (n 36), 537; Drożdż (n 62), 54–57.

64 Isak Mendoza and Lee Bygrave, 'The Right Not to be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou and Thalia Prastitou Synodinou, (eds) *EU Internet Law* (Springer 2017), 93. The CJUE has adopted a broad interpretation of 'automated individual decision-making' in the judgment of 7 December, Case C-634/21, OQ v Land Hessen, ECLI:EU:C:2023:957, para. 73.

65 Čertický (n 19), 45.

self is lawful under Article 6 GDPR alone or Article 6 GDPR in conjunction with Article 9 GDPR, they have to obtain additional consent from the data subject for the automation of data processing.[66]

However, the above requirement does not apply if automated individual decision-making is necessary for entering or performing a contract between the data subject and a data controller, or is authorised under EU or national law to which the controller is subject,[67] and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.[68] In the light of the above, in some instances, automation of the underwriting process might be allowed based on national law, while in others it is necessary to examine if automated individual decision-making was necessary for entering or performing a contract between the data subject

66 This applies to real-time, continuous data recording concerning the insured consumer as a data subject, Čertický (n 19), 48. See also EDPB (2020) *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*.

67 See, under Polish law, Article 41 of the Act on Insurance and Reinsurance Business of 11 September 2015 (Law Journal of 2023, item 656) which states that:
Section 1a. The insurance company may make decisions in individual cases based solely on automated processing, including profiling, of personal data in order to:
1) assess the insurance risk – in the case of personal data relating to the insured persons,
2) performance of insurance activities referred to in Article 4 Section 9 points 1 and 2 – in the case of personal data relating to the insured, policyholders and persons entitled under the insurance contract
– provided that the person affected by the automated decision is given a right to receive appropriate explanations as to the basis for the decision, to protest the decision, to express his or her position and to obtain human intervention.
Section 1b. The decisions referred to in section 1a, may be made only on the basis of the following categories of data relating to a natural person: 1) name(s) and surname; 2) family name; 3) parents' names; 4) date and place of birth; 5) age; 6) gender; 7) citizenship; 8) PESEL number, if assigned; 9) tax identification number, if assigned; 10) number and series of ID card or other document confirming identity; 11) nature of work performed (sector); 12) place of residence; 13) insurance period; 14) insurance history; 15) sum insured; 16) marital status; 17) health condition of the insured person; 18) financial situation; 19) date and number of damage registration, date of damage occurrence, and date of reporting the damage or claim; 20) identifying the insurance contract to which the damage relates; 21) identifying the subject of insurance; 22) the number, type and dates of offenses or crimes constituting violations of road traffic regulations, including driving under the influence of alcohol or under the influence of alcohol or substances acting similarly to alcohol; 23) the number of points assigned to violations of road traffic regulations referred to in point 22, and the amount of fines imposed by way of a penalty notice and the fact of their payment.

68 Bygrave (n 63), 536-538; Čertický (n 19), 48-49.

(the consumer) and the data controller (the insurance distributor).[69] One should remark with caution that there appears to be no clarification as to how this criterion of 'necessity' should apply in practice, so it is ultimately left to courts to determine.[70] Nonetheless, the criterion of 'necessity' cannot be fulfilled where the personalisation of insurance contracts is not mandated by law but merely results from the commercial practices of insurance distributors.

III. Information duties on data processing under GDPR

Since the approach of EU law towards data processing is based on the consent-notice model, the information duties of data controllers form an important part of the GDPR.[71] Consequently, an insurance distributor as a data controller is required to inform the data subject about the processing of their personal data regardless of whether personal data is obtained from the data subject (Article 13 GDPR) or an external source (Article 14 GDPR). Information duties imposed under Article 13 GDPR must be fulfilled when personal data is collected, not after that, and also every time personal data is gathered.[72] When personal data is collected from an external source, then information duties are to be fulfilled in a reasonable time, no later than one month after the data has been collected.[73]

Information that must be provided includes the identity and contact details of the controller and, where applicable, of the controller's representative, the contact details of the data protection officer. Furthermore, the purposes of the processing for which personal data is intended need to be indicated as well as the legal basis for the processing and other matters set out in Article 13(1), Article 13(2), Article 14(1), and Articles 14(2) GDPR. Information about the purposes of processing is particularly important as exceeding the scope of the specified processing purposes, and herewith

69 Cf. in detail Čertický (n 19), 41-42.
70 Soyer (n 15), 175, observes that it is unlikely that the criterion of being 'necessary' connotes indispensability.
71 Thouvenin, Suter, George and Weber (n 4), 227.
72 Gabriela Zanfir-Fortuna, 'Commentary to Article 13 GDPR' in Kuner, Bygrave, Docksey and Drechsler (n 36), 425–427; Rossana Ducato, 'Data protection, scientific research, and the role of information' (2020) Computer Law and Security Review, 10.
73 Zanfir-Fortuna (n 72), 445; Ducato (n 72), 10.

diverging from the initial purpose of processing infringes on Article 5(b)(1) GDPR.[74]

With respect to personal data processing within the framework of automated decision-making mechanisms, data controllers are obliged under the provisions of Articles 13(2)(f), 14(2)(g), and (15)(1)(h) GDPR to inform data subjects not only about the use of automated decision-making in personal data processing but also about the logic (assumptions) behind this mechanism.[75] However, the nature of this information duty is debated; specifically, it is contentious whether this duty can only be fulfilled *ex-ante* or also *ex-post*.[76]

In practice insurance distributors usually process large sets of personal data of insurance consumers for different purposes; the legal bases for that processing tend to differ in the context of each of these purposes. This alone makes it difficult to fulfil information obligations as achieving sufficient transparency of information is a challenge.

D. Personalised pricing of insurance products under Unfair Commercial Practices Directive

Under EU law, business conduct involving price personalisation in relation to consumers is subject to the assessment under the Unfair Commercial Practices Directive. The main objective of the Unfair Commercial Practices Directive is to protect consumers from the consequences of unfair commercial practices which could 'directly harm consumers' economic interests and thereby indirectly harm the economic interests of legitimate competitors'.[77] Most importantly, UCPD protects consumer economic interests from unfair business-to-consumer commercial practices and addresses commercial practices directly related to influencing consumers' transactional decisions concerning products.[78] It follows that market practices of an insurance distributor that involve processing personal data under GDPR are subject

74 Zanfir-Fortuna (n 72), 430.
75 Mendoza and Bygrave (n 64), 93; Jonas Knetsch, 'Data Protection Rights and Automated Decision-Making in the Field of Insurance' in Cristina Poncibò and Piotr Tereszkiewicz (eds), *The Evolution of European Insurance Contract Law in the Digital Age* (Springer forthcoming), passim; Rott, Strycharz and Alleweldt (n 21), 27.
76 Mendoza and Bygrave (n 64), 93-94.
77 See recital 6 UCPD.
78 Idem.

to control under UCPD, if they harm the economic interest of consumers by influencing their transactional decisions. There are three consecutive tests for assessing whether a commercial practice may be considered unfair under UCPD.[79]

The first test is performed by analysing whether a relevant practice falls within the blacklist of unfair commercial practices annexed to UCPD. If this is the case, then such a practice is unconditionally regarded as unfair.[80] The second test requires an assessment of whether a relevant practice is misleading by action (Article 6 UCPD) or omission (Article 7 UCPD), or is aggressive (Article 8 UCPD).[81] Finally, there is an assessment of unfairness under the general clause of Article 5 UCPD: a commercial practice is unfair if 'it is contrary to the requirements of professional diligence' and it 'materially distorts or is likely to materially distort the economic behaviour about the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers'. To pass the fairness test of Article 5 UCPD, a commercial practice must satisfy both criteria laid down by this provision.

Under the above framework, establishing whether a trader's conduct involving personalising insurance prices contrary to GDPR qualifies as an unfair market practice requires the examination of the blacklist of unfair market practices as laid down in Annex I to Directive 2005/29/EC. Annex I contains commercial practices divided into two groups: misleading and aggressive.[82] Personalisation conducted in a manner inconsistent with GDPR

79 Jules Stuyck, Evelyn Terryn and Tom van Dyck, 'Confidence Through Fairness? The New Directive on Unfair Business-To-Consumer Commercial Practices in the Internal Market' (2006) 43 CMLRev, 132-134; Hans-Wolfgang Micklitz, 'The general clause on unfair practices' in Geraint Howells, Hans-Wolfgang Micklitz and Thomas Wilhelmsson (eds) *European Fair Trading Law The Unfair Commercial Practices Directive* (Routledge Taylor & Francis Group 2016), 85-86; Guidance on the interpretation and application of Directive 2005/29/EC (2021), 26.

80 Hans-Wolfgang Micklitz, 'Unfair commercial practices and misleading advertising' in Hans-Wolfgang Micklitz, Norbert Reich and Peter Rott, *Understanding EU Consumer Law* (Intersentia 2009), 88-89; Geraint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking Eu Consumer Law* (Routledge Taylor & Francis Group 2018), 53.

81 Monika Namysłowska, 'Dziesięć lat dyrektywy 2005/29/WE o nieuczciwych praktykach handlowych' (2016) 3 Europejski Przegląd Sądowy, 5.

82 Micklitz (n 80), 111; Jules Stuyck, 'The Court of Justice and the Unfair Commercial Practices Directive' (2015) Common Market Law Review, 741; Howells, Twigg-Flesner and Wilhelmsson (n 80), 53.

is not included in the blacklist as such. Moreover, non-compliance with GDPR itself does not qualify as an example of blacklisted market practices. It appears that the first test of unfairness may be passed: personalising insurance prices without complying with GDPR does not qualify as one of the unfair commercial practices listed under Annex I.

However, it is important to observe that an amendment to Annex I has been recommended in the BEUC Report.[83] *Inter alia* adding the following practices was proposed:

> '(49) Practices including behavioural (algorithmic) pricing, as well as those involving personalised pressure, performed based on detailed profiles mapping a person's personality, biases and vulnerabilities (psychographic profiles) should always be deemed as unfair.
> (50) Similarly, digital commercial practices should be prohibited where they are using data which may reasonably be suspected to have been obtained in breach of data protection laws.'

This proposal merits attention given the dual character of its approach. Under Point (49) of the BEUC Report, prohibiting some of the sophisticated market practices based on and inextricably linked with personal data processing regardless of whether they are performed with the breach of GDPR has been recommended. The main justification relates to the concern that personalisation based on mapping one's personality, biases and vulnerabilities has an immense potential to distort consumer market behaviour in a manner that is unperceivable for the data subject when they consent to data processing. In contrast, under Point (50) of the BEUC Report, the sole fact that it may be reasonably suspected that data processed within the framework of a digital commercial practice has been obtained in breach of GDPR automatically leads to the qualification of such a commercial practice as unfair. It follows that a potential[84] breach of GDPR at the data-gathering stage 'poisons' all digital commercial practices that are undertaken using that data. Consequently, on this account practices involving any potential breach of GDPR would be considered to be unfair. A possible justification for such a robust approach would be that in the digital environment, it is very difficult to assess whether personal data were gathered in compliance with data protection laws, i.e., whether a data subject has been properly

83 *EU Consumer Protection 2.0. Protecting fairness and consumer choice in a digital economy* (BEUC 2022), 12.

84 It is sufficient that a breach can be reasonably supposed.

informed about the purpose of data processing. One could thus claim that for the prohibition to be effective in practice, the occurrence of a breach of GDPR does not have to be established, but only reasonably suspected.

The second test of unfairness under UCPD includes two steps.[85] First, it needs to be examined whether processing personal data in breach of GDPR can qualify as an aggressive practice, and second – if a breach of GDPR can be classified as a misleading practice. In both instances, one must establish whether the practice at hand causes or is likely to cause the consumer to make a transactional decision that he or she would not have taken otherwise.

Under Article 8 UCPD, a commercial practice shall be regarded as aggressive if, by harassment, coercion, including the use of physical force, or undue influence (Article 9 UCPD), it significantly impairs or is likely to significantly impair the consumer's ability to make a conscious decision,[86] in a manner that affects or is likely to affect his or her market behaviour, causing him to take a transactional decision that he would not have taken otherwise.

In principle, the personalisation of insurance prices itself cannot be classified as an aggressive commercial practice:[87] Adjusting the price of insurance products using processing personal data cannot be seen as significantly impairing – or being likely to significantly impair – consumers' freedom of choice by harassment, coercion, including the use of physical force, or undue influence. One can imagine a situation whereby an insurance distributor infringes on GDPR in order to cause a consumer to buy an insurance product. Specifically, using personal data, a trader can learn about sudden changes in the life of a consumer (e.g., the death of a family member, serious illness) and use this knowledge to exercise mental pressure to cause that consumer to buy an insurance product where the price is personalised. This would amount to exploiting '(...) specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision about the product' under Article 9(c) UCPD. Nonetheless, what makes such a

85 Howells, Twigg-Flesner and Wilhelmsson (n 80), 57-58.

86 Micklitz (n 80), 86; Mariusz Golecki and Piotr Tereszkiewicz, 'Taking the Prohibition of Unfair Commercial Practices Seriously' in Klaus Mathis, Avishalom Tor (eds), *New Developments in Competition Law and Economics. Economic Analysis of Law in European Legal Scholarship*, vol *7* (Springer 2019), 91.

87 Bourreau and de Streel (n 6), 6, claim it is currently unclear under which circumstances personalised prices can be considered an unfair commercial practice.

practice an aggressive commercial practice under UCPD is neither price personalisation nor a GDPR breach *per se*, but rather the fact that in such cases the requirements of Article 8 UCPD are met. There are undoubtedly cases where a commercial practice will, at the same time, infringe on GDPR and be considered aggressive under Article 8 UCPD; but this does not necessarily entail that it is a GDPR breach that makes such a practice an aggressive market practice.

Further, Articles 6 and 7 of UCPD introduce a specific prohibition of misleading commercial practices. Specifically, Article 6(1) UCPD prohibits commercial practices containing false information that are, therefore, untruthful or in any way, including overall presentation, deceive or are likely to deceive an average consumer, even if the information is factually correct. In principle, misleading information should concern the existence or nature of the product, its main characteristics, price, maintenance, the trader, or consumer rights.[88]

Article 6(1)(d) UCPD has a significant function for the assessment of whether price personalisation practices are allowed: it prohibits practices that mislead or are likely to mislead a consumer, even if they contain the factually correct information, on price or its calculation method – without limitation to the subject matter on which the price is determined. Thus, the use of personalised discounts or overpricing insurance products based on certain personal data may be considered misleading in cases where consumers are misinformed as to how insurance premiums and related costs were calculated.[89] Specifically, an insurance distributor may inform the consumer that the insurance price was tailored for them (or even specify that this personalisation was performed in the consumer's interest), while in reality what the insurance distributor, when setting the prices, takes into account is whether the device the consumer is using has a Microsoft operating system or macOS.[90] The objective of such a practice would be to artificially increase prices offered to consumers who are macOS users. One could argue that here a breach of GDPR and a misleading character of the market practice are just coincidental. Nonetheless, in virtually all scenarios where personalised pricing infringes on GDPR, the consumer

88 Howells, Twigg-Flesner and Wilhelmsson (n 80), 63.

89 Alexandre de Streel and Florian Jacques, 'Personalised pricing and EU law' in 30th European Conference of the International Telecommunications Society (ITS): 'Towards a Connected and Automated Society', Helsinki, Finland, 16th-19th June 2019 (International Telecommunications Society (ITS) 2019), 5.

90 Similar examples are indicated by Bourreau and de Streel (n 6), 3.

will be misled as to the price or how the price is calculated. This is because the price-related information that is provided to the insurance consumer may cause them to believe that all the data processing, performed within the price calculation, was lawful.

Moreover, a commercial practice shall also be regarded as a misleading omission within the meaning of Article 7 UCPD when a trader (insurance distributor) does not provide a consumer with all the material information necessary to make a well-informed decision and hereby causes or is likely to cause the average consumer to take a transactional decision that he or she would not have taken otherwise. In general, one can assume that information about the price and its personalisation is crucial for any consumer.[91] This is especially the case if the personalisation of price takes place using fully automated decision-making and a contract is concluded at a distance: in such cases Article 6(1)(ea) of the Consumer Rights Directive[92] might be applicable. Under this provision, a trader is obliged to inform the consumer in a clear and comprehensible manner that the price has been individually adjusted based on automated decision-making.[93] However, financial services are excluded from the scope of the Consumer Rights Directive since they are subject to comprehensive regulation in sector-specific acts at the EU level.[94] Yet remarkably, a provision on price personalisation, comparable to the one of Article 6(1)(ea) Consumer Rights Directive, cannot be found in the Directive 2002/65/EC concerning the distance marketing of consumer financial services.[95] Should one consider this legislative choice

91 Cristina Poncibò and Rossella Incardona, 'The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) 30 Journal of Consumer Policy, 31; *Fitness check of EU consumer law* (BEUC 2017), 5; *Ensuring consumer protection in the platform economy* (BEUC 2018), 9.

92 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L 304/64 (referred to as Consumer Rights Directive, CRD).

93 Rott, Strycharz and Alleweldt (n 21), 28–29. For a sceptical view of this provision, see Jabłonowska, Lagioia and Sartor (n 53), underlining that the impact of this provision may in practice depend on its interpretation, and the latter is disputed.

94 See Article 3(3)(d) Consumer Rights Directive, and contributions in Veerle Colaert, Danny Busch and Thomas Incalza (eds), European Financial Regulation Levelling the Cross-Sectoral Playing Field (Bloomsbury 2019); Golecki and Tereszkiewicz (n 86).

95 Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services [2002] OJ

meaningful, it would weigh against the interpretation that a failure to inform about the personalisation of insurance prices constitutes a misleading commercial practice under Article 7 UCDP.

Still, one could argue that – in the case of the personalisation of insurance prices – all the information that should be provided under GDPR should be regarded in the light of Article 7(5) UCPD as material within the meaning of Article 7(1) UCPD. A possible argument could run as follows: the provision of Article 7(5) UCPD suggests that information requirements established under EU law concerning commercial communications, including advertising or marketing, indicate what information should be considered material in this context. The catalogue of regulatory acts that should be taken into account is found in Annex II to UCPD. Given this list has merely a non-exhaustive, indicative nature, it is submitted that even though GDPR is not included in it, information obligations under GDPR should be considered material under UCPD. We argue that within the data-driven EU market economy, the relevance of data, including personal data, has been greatly increasing. Data has become a commodity, a factor shaping market strategies and behaviours.[96] These factual developments should be reflected by recognizing that data-related information obligations, such as those found in GDPR, form part of the core legal framework on mandatory consumer information under EU law. Under this view, the information duties that a data controller has to a data subject play an important role in shaping consumer digital literacy in the context of commercial communication including advertising or marketing. It follows that information obligations stemming from GDPR can be considered 'information requirements relating to commercial communication' including advertising or marketing within the meaning of Article 7(5) UCPD.

Further, one should consider the related question of whether an omission by a trader to provide information on the personalisation of insurance pricing causes or is likely to cause an average consumer to make a transactional decision that he or she would not have taken otherwise. In analysing

---

L 271/16. The EU legislator should, however, reconsider introducing the obligation to inform the consumer that the price has been individually adjusted based on automated decision-making in a clear and comprehensible manner also in the case of distance contracts for financial services. A revision of Directive 2002/65/EC is currently taking place.

96 The Geneva Association: Report Big Data and Insurance: Implications for innovation, competition and privacy (2018); Thouvenin, Suter, George and Weber (n 4), 227-230; Soyer (n 15), 166-167.

this question, one should point out that the personalisation of insurance prices, similar to the personalisation of prices on different markets, may lead to higher prices for certain consumers and lower prices for others. Consequently, some consumers may not want to purchase the product from a given trader in the knowledge that they can buy it cheaper from a different trader who does not personalise their prices.[97] Other consumers, for whom personalisation might result in paying lower premiums for the same insurance cover, may seek personalised offers. One could thus assume that a trader's omission to inform customers about the personalisation of insurance prices is likely to lead a consumer to make a transactional decision that he or she would not have made knowing that the price of the insurance product offered is determined in the process of digital personalisation.[98]

Moreover, what is interesting in the context of misleading omissions is that they are likely to coincide with GDPR infringements by a trader. Insurance distributors, who fail to inform insurance consumers that insurance prices are personalised, may also fail to ensure that consumers' personal data are processed in full compliance with GDPR. In particular, insurance distributors may omit to inform consumers as data subjects under GDPR about the specific purpose of personal data processing and the automated decision-making employed in the product distribution.

Assuming that a commercial practice passes the tests of Article 6 and 7 UCPD, it may still be subject to review as to unfairness under Article 5(2) UCPD, which serves as a safety net for consumers.[99]

Under Article 5(2) UCPD, which is labelled the general clause, a commercial practice shall be regarded as unfair if it is contrary to the requirements of professional diligence and it materially distorts or is likely to materially distort the economic behaviour (concerning the product) of the average consumer. The first question that should be answered in this context is whether the practice can be regarded as contrary to the requirements of diligence if it is based on processing personal data in a manner contrary to GDPR provisions. The requirements of professional diligence are understood as the standard of care that a trader may reasonably be

97 de Streel and Jacques (n 89), 5.

98 Introducing an explicit duty for traders to inform consumers about price personalisation and the main parameters used for the personalisation is recommended by Bourreau and de Streel (n 6), 11, with reference to OECD (2018).

99 Micklitz (n 80), 89; Stuyck, Terryn and van Dyck (n 79), 106; Howells, Twigg-Flesner and Wilhelmsson (n 80), 58.

expected to exercise towards consumers.[100] Traders who undertake activities that include the processing of personal data of consumers, including personalisation – or as in the case at hand: the personalisation of insurance prices – can reasonably be expected to comply with GDPR while processing that data. This implies that processing the personal data of consumers while infringing on GDPR requirements should be considered a commercial practice that is contrary to the requirements of professional diligence.

However, for a commercial practice to be regarded as unfair under Article 5(2) UCPD, further requirements must be met. In this context, it needs emphasising that not every (potential) distortion of consumer behaviour is automatically regarded as fulfilling the second premise of Article 5(2) UCPD. The distortion must be material, which means that a commercial practice must show sufficient impact to impair the consumer's ability to make decisions[101] and have the potential to affect the consumer's market behaviour. By contrast, insignificant instances of misconduct by traders do not qualify as leading to material distortions.[102] An informational advantage that traders necessarily have over consumers is not sufficient in itself to distort or have the potential to distort the average consumer's market conduct.[103] What is additionally required is an exploitation of the informational advantage by a trader (an insurance distributor) to the detriment of a consumer. Given the reality of digital mass-markets establishing whether personalising practices may materially distort consumers' behaviour may be difficult.[104]

100 Micklitz (n 80), 85; Howells, Twigg-Flesner and Wilhelmsson (n 80), 58-60.

101 Micklitz (n 80), 86–87. It is important to distinguish between an unfair commercial practice designed to influence a consumer's decision, basically leaving the consumer with no freedom of choice, and nudging, which is designed to induce a choice, but with a strong emphasis on full freedom of choice, see Avishalom Tor, 'The Critical and Problematic Role of Bounded Rationality' in Klaus Mathis and Avishalom Tor (eds.) *Nudging. Possibilities, Limitations and Applications in European Law and Economics* (Springer 2016), 4-7.

102 Hugh Collins, 'Harmonisation by Example: European Laws against Unfair Commercial Practices' (2010) 73 Modern Law Review, 101.

103 For more on the impact of new technology tools on the autonomy of contracting parties see Mik (n 2), 1-38.

104 Południak-Gierz (n 51), 172-173.

E. Infringement of GDPR as an unfair commercial practice?

The Chapter has so far discussed the interplay between GDPR and UCPD and spelt out typical circumstances in which an infringement of GDPR can be regarded as one of the factors leading to the unfairness of a commercial practice within which GDPR infringement occurred. In the next step, one could go even further and consider whether an infringement of GDPR itself could be considered an unfair commercial practice under UCPD. Recognising that an infringement of GDPR automatically justifies finding a commercial practice unfair under UCPD could substantially improve the legal situation of consumers who buy products as a result of personalisation practices and find that personalisation was executed without compliance with GDPR. Specifically, the consumer then could invoke remedies granted under Article 11a UCPD, i.e., claiming compensation, terminating the contract, or reducing the scope of their obligation.

The possibility of applying a similar 'shortcut' argument in order to ascertain one's rights was discussed in the CJEU *Pereničová* judgment.[105] There, the Court was confronted with the question of whether a finding that a commercial practice of using contractual terms that could mislead consumers as to the scope of their rights and obligations was unfair influences (or possibly even determines) the outcome of the assessment of whether these terms are to be considered unfair under Article 4(1) of the Unfair Contract Terms Directive (UCTD).[106]

The Court initially found that:

> 'A commercial practice such as that at issue in the main proceedings which consists in indicating in a credit agreement an APR lower than the real rate constitutes false information as to the total cost of the credit and hence the price referred to in Article 6(1)(d) of Directive 2005/29'.[107]

Based on the above finding the Court subsequently concluded that:

> 'A commercial practice such as that at issue in the main proceedings which consists in indicating in a credit agreement an annual percentage

105 Judgment of the Court (First Chamber), 15 March 2012, Jana Pereničová and Vladislav Perenič v SOS financ spol. s r. o., Case C-453/10, ECLI:EU:C:2012:144.

106 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29.

107 Judgment of the Court (First Chamber), 15 March 2012, Jana Pereničová and Vladislav Perenič v SOS financ spol. s r. o., Case C-453/10, ECLI:EU:C:2012:144, para. 41.

> rate of charge lower than the real rate must be regarded as "misleading" within the meaning of Article 6(1) of Directive 2005/29/EC [...] in so far as it causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise. [...] A finding that such a commercial practice is unfair is one element among others on which the competent court may, pursuant to Article 4(1) of Directive 93/13, base its assessment of the unfairness of the contractual terms relating to the cost of the loan granted to the consumer. Such a finding, however, has no direct effect on the assessment, from the point of view of Article 6(1) of Directive 93/13, of the validity of the credit agreement concluded.'[108]

The Court thus took the view that finding that a commercial practice of using a specific contract term meets the test of unfairness under UCPD is merely one of the factors to be taken into account in the assessment as to whether contract terms are at the same time unfair under the Unfair Contract Terms Directive. While the requirements provided under both the Directives in question should thus be examined independently of each other, the outcome of the assessment under the Unfair Contract Practices Directive retains relevance for the assessment under the Unfair Commercial Terms Directive.

Another issue is whether the same manner of reasoning should be applied when a term in a consumer contract is deemed unfair. As discussed above, one could assume that the inclusion of a such a term in consumer contracts should not automatically amount to an unfair commercial practice within the meaning of UCPD. Nevertheless, the unfair character of the contract term that is used by the trader should be considered when the fairness of a commercial practice (which includes using this contract provision) is assessed. This appears justified in cases where unfair contract terms in question do not meet the transparency requirement under UCTD. This is because it is the lack of transparency that makes the consumer prone to overlook a significant imbalance in the parties' rights and obligations created by the unfair term. It prevents the consumer from taking an informed transactional decision and, thereby, causes or is likely to cause the average consumer to take a transactional decision that he or she would not have taken otherwise.

108 Idem, para. 47.

Formally, the same approach should be applied in analysing the relationship between the Unfair Commercial Practices Directive and GDPR. It suggests that while a breach of GDPR should be considered an important factor when assessing the unfairness of a commercial practice under the Unfair Commercial Practices Directive, it does not, by itself, constitute an unfair commercial practice.

Further, a similar position in favour of the complementary character of the EU consumer protection provisions on the one hand and data protection provisions on the other hand was taken in the European Commission's Staff Working Document. There, it is claimed that the violation of data protection rules does not always mean that the practice would be regarded as unfair under UCPD, yet such data protection violations should be considered when assessing the overall unfairness of commercial practices under UCPD, particularly in the situation where the trader processes consumer data in violation of data protection requirements, i.e., for direct marketing purposes or any other commercial purposes such as profiling, personal pricing or big data applications.[109]

F. Conclusions

This Chapter aims at providing insights into the complex and yet unexplored interplay between GDPR and UCPD in the context of the personalised pricing of insurance products. As the law stands now, infringements of GDPR or the personalisation of prices (both in general and specific sectors) are not listed in Annex I to UCPD. The case, which the BEUC report makes for extending the blacklist of unfair commercial practices by including certain forms of infringement of GDPR, appears largely justified. Amendments proposed by BEUC would strengthen the protection of consumers' personal data since practices included in the blacklist are considered unconditionally unfair. Introducing such measures would be a particularly suitable response in cases where traders intentionally violate GDPR during personal data processing to be able to personalise the prices of insurance products.

109 European Commission (2016), Staff Working Document of 25 May 2016 on Guidance on the implementation/application of the Directive 2005/29 on Unfair Commercial Practices, SWD(2016) 163, 26.

Further, the Chapter has shown that there are cases of price personalisation of insurance products that do not comply with GDPR requirements and can be regarded as misleading commercial practices both under Article 6 and Article 7 UCPD. One should not regard such scenarios as being isolated and purely coincidental since misleading commercial practices that use personalisation are usually preceded by major GDPR breaches. Moreover, the analysis revealed several challenges posed by the automation of decision-making processes in product distribution within the insurance sector. Assuming that a similar level of protection should be granted to consumers both in financial services and other markets, one should recommend generalising the regulatory objective of Article 6(1)(ea) Consumer Rights Directive and imposing on traders the obligation to inform consumers about price personalisation when providing financial services, including insurance.[110] Tailored regulation of the information duties concerning automatic decision-making mechanisms requires a high degree of coherence between provisions on data protection, financial services, and consumer law.

Moreover, commercial practices undertaken in breach of GDPR can reasonably be seen as contrary to the requirements of professional diligence. However, for such practices to be regarded as unfair commercial practices under the UCPD, the assessment depends on whether the practice at hand also materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer.

Given the complexity of the subject matter herein analysed, and the evident digital vulnerability[111] of a contracting party who is both a consumer and a data subject under GDPR, one might be tempted to advocate a 'shortcut' solution, under which a breach of GDPR automatically constitutes an unfair commercial practice under the UCPD in cases of the personalised pricing of insurance products. A better view is to resist this urge and assume

110 See also Bourreau and de Streel (n 6), 11; OECD 2018; similarly Poncibò (n 7), 336.

111 Kasper Drazewski, *EU Consumer Protection 2.0. Protecting fairness and consumer choice in a digital economy*, (BUEC 2022) <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf>: '… in digital marketplaces, most if not all consumers are potentially vulnerable. Instead of singling out certain groups of consumers, digital vulnerability describes a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, "datafied" consumer-seller relations and the very architecture of digital marketplaces'.

that the two regulatory regimes are independent but open for mutual influences.

Ideally, the extent to which insurance contracts can be personalised (individualised) should be determined by specific provisions of (insurance) law, preferably adopted following a public dialogue involving all stakeholders.[112] Determining which sectors of insurance should be governed by the principle of solidarity and which may be governed by the personalisation of insurance contracts will be a complex process needing time. For the time being, data protection law and consumer law will continue to play an important role in setting the limits for the market conduct of insurers.

112 Thouvenin, Suter, George and Weber (n 4), 243.