Big Data in the Insurance Industry

Leeway and Limits for Individualising Insurance Contracts

by **Florent Thouvenin[*], Fabienne Suter[†], Damian George[‡] and Rolf H. Weber[§]**

Abstract: With the advent of big data analytics, the individualisation of mass market insurance policies has become commercially attractive. While this development would have positive economic effects, it could also undermine the principle of solidarity in insurance. This paper aims to outline the different regulatory approaches currently in place for dealing with this fundamental challenge by analysing the insurance, anti-discrimination and data protection laws of Switzerland and the U.S./California pertaining to health, renters and automobile insurance. It will be shown that the leeway for individualising insurance contracts is vanishingly small for (mandatory) health insurance on both sides of the Atlantic. By contrast, the two legal systems pursue different regulatory approaches with regard to the other two types of insurance. Renters and automobile insurance are predominantly governed by the freedom of contract principle in Switzerland, whereas in California sector specific regulations significantly limit the informational basis of insurance companies, thereby limiting the leeway for individualisation to a large extent. While Swiss anti-discrimination law hardly restricts the individualisation of insurance contracts, U.S. and California law prohibit such individualisation based on protected characteristics, in this way further restricting the remaining leeway. While privacy laws in the U.S. and California set some significant but rather specific limits for the individualisation of insurance contracts based on the use of personal data, the all-encompassing Swiss (and European) data protection law is clearly the most important barrier to individualisation in Switzerland. Namely, it remains unclear whether the processing of personal data for the purpose of individualising insurance contracts may be based on the legitimate interests of the insurer. As a consequence, insurance companies are advised to always obtain their customers' consent for making individual offers based on big data analytics. The authors conclude that instead of indirectly hindering the individualisation of insurance contracts through data protection law, Swiss (and European) lawmakers should initiate a dialogue involving all stakeholders to determine which sectors of insurance should be dominated by the principle of solidarity and in which sectors and on what informational basis the individualisation of insurance contracts should be allowed.

Keywords: Individualisation; Big Data; Insurance Contracts; Insurance Law; Discrimination; Data Protection Law

Recommended citation: Florent Thouvenin, Fabienne Suter, Damian George and Rolf H. Weber, Big Data in the Insurance Industry: Leeway and Limits for Individualising Insurance Contracts, 10 (2019) JIPITEC 209 para 1.

A. Introduction

1 The individualisation of insurance contracts is not an entirely new phenomenon, but it has long been quite costly and, therefore, not very widespread. By definition, insurance is a data-rich industry; the insurance undertakings always had to base their business on accurate and relevant data for risk-based calculations.[1] The growing amount of data (big data), the increasing computing power and novel technologies (big data analytics), however, allow today's insurance companies to individualise insurance contracts in all sectors of the industry.

2 In most insurance markets, companies have long operated with categories of insured for which they calculated the risks and the corresponding premiums. But due to big data analytics, it has recently become commercially viable to create risk profiles for individual customers and make them corresponding individual offers.[2] At least from today's perspective, this applies above all to insurance premiums. Individualisation of other contractual conditions is unlikely to be commercially attractive in the near future.

3 The individualisation of insurance premiums raises fundamental legal questions. Given that one of the basic concepts of insurance has always been (and continues to be) the solidarity of the insured,[3] the law will need to strike an appropriate balance between the opposing concepts of solidarity and individualisation. Different legal systems will come up with different solutions and these solutions will likely not be the same for all types of insurances. This paper aims to outline possible solutions to this fundamental challenge by analysing the legal situation on both sides of the Atlantic using the jurisdictions of Switzerland (incl. partly the EU) and California as examples of two quite different approaches.

4 For both systems, three bodies of law need to be analysed: First, we will clarify if and to what extent the applicable insurance regulations allow for an individualisation of insurance contracts (C). Second, we will assess whether and under what conditions the individualisation of insurance contracts is compatible with the requirements of anti-discrimination law (D). Third, we will investigate whether the processing of personal data, which is carried out to calculate individual premiums, complies with the requirements of data protection law (E). In order to gain a broad picture of the phenomenon, we will analyse three types of insurances: (mandatory) health insurance, renters insurance and automobile insurance. At first, however, we will briefly outline the rationale behind the individualisation of insurance contracts (B).

B. Individualisation of Insurance Contracts

5 Insurance contracts – and in particular insurance premiums – can essentially be individualised with regard to two aspects: the risk profile, defined by factors such as age, gender, health, work activity, place of residence, driving behaviour, etc., and the willingness to pay.[4] These two aspects can easily be combined in the individualisation of an offer. Nevertheless, the rationale for individualisation in terms of the willingness to pay differs from the rationale for individualisation with regard to the risk profile. Each aspect will therefore be discussed separately.

* Professor of Information and Communications Law, Chair of the Executive Board of the Center for Information Technology, Society, and Law (ITSL), and Director of the Digital Society Initiative (DSI) University of Zurich, Switzerland.

† Ph.D. cand., University of Zurich, Switzerland.

‡ Ph.D. cand., University of Zurich, Switzerland.

§ Professor of Law emeritus, Member of the Executive Board of the Center for Information Technology, Society, and Law (ITSL), University of Zurich, Switzerland.

1 Rolf H. Weber, 'Big Data in the Insurance Industry' (2016) Jusletter dated 12 December 2016, para 3.

2 Cf. IBM Corporation, Harnessing the power of data and analytics for insurance (White Paper, 2015) 2; PricewaterhouseCoopers, Der Insurance Monitor: Operational Excellence - Analytics als Grundlage für ein digitales Geschäftsmodell, June 2016, <https://news.pwc.ch/de/28303/studie-der-insurance-monitor-operational-excellence-analytics-als-grundlage-fur-ein-digitales-geschaftsmodell/> accessed 25 September 2018, at 18 ff.; BearingPoint Institute, 'The smart insurer: more than just big data', <www.bearingpoint.com/files/BEI004-17-The-smart-insurer.pdf&download=0&itemId=389133>, accessed 25 September 2018, 58; Philip Bitter and Steffen Uphues, 'Big Data für die Versichertengemeinschaft', in: Thomas Hoeren (ed) Phänomene des Big-Data-Zeitalters: Eine rechtliche Bewertung im wirtschaftlichen und gesellschaftlichen Kontext, (Westfälische Wilhelms Universität Münster 2019) 147, 153 f.; Weber (n 1) para 8ff. For times when such individualisation was not yet possible cf: Willy Koenig, Schweizerisches Privatversicherungsrecht: System des Versicherungsvertrags und der einzelnen Versicherungsarten (Herbert Lang & Cie 1967) 172.

3 E.g. Weber (n 1) para 16.

4 Moreover, prices might be individualised based on the likelihood that a policyholder will change carriers, see: Rick Swedloff, 'Regulating Algorithmic Insurance' (2019) <http://dx.doi.org/10.2139/ssrn.3346753>, accessed 8 April 2019, 4.

I. Risk Profile

6 Insurance premiums are generally calculated based on the risk profile of the insured. Most often, however, insurance companies do not calculate the risk for each customer but form groups of customers and offer premiums corresponding to the risk assessment of that group. This serves two important policy goals; namely, the reduction of adverse selection and the avoidance of moral hazard.

7 The notion of adverse selection[5] refers to the phenomenon that more attractive suppliers or buyers are driven out of the market due to information asymmetries. If insurance companies were to insure a certain risk for all potential policyholders at a uniform price, taking out such insurance would be particularly attractive for persons whose individual risk is above the average risk on the basis of which the uniform premium was calculated. The offer would therefore attract comparatively unattractive customers. If only these customers were to take out the insurance offered, the insurance company would either have to accept losses because the risks associated to its customers are higher than anticipated, or it would have to increase the premiums in order to reflect the higher risks of its actual customers. Over time, this mechanism would, theoretically, increase the premiums to a point where it would no longer be worthwhile for anyone to take out insurance. In reality, however, this effect is unlikely to be observed because policyholders are unable to assess their risks accurately; rather, they are prepared to take out insurance against a risk that cannot be precisely calculated. Even if the mechanism described is hardly observed in practice, a uniform premium for all policyholders would still attract comparatively unattractive customers and may thus lead to a race to the bottom. The formation of risk groups can prevent this effect by offering insurance to members of different risk groups at different prices. This is all the more true if the offers are individualised according to the risk profile of the individual policyholders.

8 Moral hazard[6] occurs when people behave irresponsibly or recklessly due to false incentives.[7] The standard example of moral hazard is a change in behaviour following the conclusion of an insurance contract for a particular risk.[8] The risk of such behavioural changes can be reduced if premiums are increased after a claim and thus incentives are created for policyholders to prevent the occurrence of a claim despite the existence of an insurance contract. The individualisation of insurance contracts – and in particular of insurance premiums – opens up further possibilities for combating moral hazard. In particular, insurers can create incentives for risk-reducing behaviour by collecting data about the behaviour of their policyholders, for example, by granting discounts if an insured person demonstrably is a cautious driver or exercises regularly.[9] These effects are positive, not only for policyholders and insurers, but also for society as a whole, since they prevent the occurrence of damage and promote the health of policyholders.[10]

9 In addition to fighting adverse selection and moral hazard, adjusting insurance premiums to the risks of individual customers or groups of customers promotes fairness by avoiding or at least limiting situations in which individuals have to pay for the risks created and the damages caused by others. It seems, however, that this only holds true for risks that can be controlled by the individual customers, e.g. by adjusting their driving behaviour. With regard to factors beyond the control of individuals – such as their genetic disposition – it would seem rather unfair if individual customers were treated differently.[11] As we will see, this distinction is already mirrored in the law to a large extent as the leeway to individualise insurance premiums is very limited for health care,[12] while it is predominantly permitted for other types of insurance such as renters insurance[13] and automobile insurance.[14]

5 On adverse selection see also: Ronen Avraham and others, 'Understanding Insurance Antidiscrimination Laws' (2014) 87 S.Cal.L.Rev 195, 204ff. with further references; Bitter and Uphues (n 2) 155.

6 On moral hazard see also: Avraham and others (n 5) 206ff. with further references; Bitter and Uphues (n 2) 156.

7 Cf. N. Gregory Mankiw and Mark P. Taylor, *Grundzüge der Volkswirtschaftslehre* (7th edn, Schaeffer-Poeschel 2018) 363; for a more restrictive definition see Peter Zweifel and Roland Eisen, *Versicherungsökonomie* (2nd edn, Springer 2003) 295f., according to which moral hazard exists when persons adapt their behaviour due to the existence of a contract.

8 Zweifel and Eisen (n 7) 295; see also Felix Walter Lanz, *Adverse Selection und Moral Hazard in der Privat- und Sozialversicherung*, Luzerner Beiträger zur Rechtwissenschaft, vol 77 (Schulthess 2014) 39; Martin Nell, *Versicherungsinduzierte Verhaltensänderungen von Versicherungsnehmern* (VVW GmbH 1993) 4.

9 So called "Pay How You Drive"-Model, cf. Allstate Corp. 'How Telematics May Affect Your Car Insurance', December 2018 <www.allstate.com/tr/car-insurance/telematics-device.aspx> accessed 4 June 2019; Rick Swedloff, 'Risk Classification's Big Data Revolution' (2014) 21 Conn. Insurance L.J. 339, 342 ff; Peter Maas and Veselina Milanova, 'Zwischen Verheissung und Bedrohung – Big Data in der Versicherungswirtschaft' (2014) 87 Die Volkswirtschaft, 23, 24.

10 In more detail: Maas and Milanova (n 9), 24ff.

11 Cf. Swedloff (n 4) 8ff. For a discussion on the fairness of (individualised) risk classification: Avraham and others (n 5) 203ff. and 214ff.

12 See below, for Switzerland: C.II.1; for California: C.III.1.

13 See below, for Switzerland: C.II.2 ; for California: C.III.2.b).

14 See below, for Switzerland: C.II.2; for California: C.III.2.c).

II. Willingness to Pay

10 Individualisation according to the willingness to pay is based on the fact that policyholders with a uniform risk profile may have a different need for insurance coverage and different financial resources for concluding an insurance contract. Insurance companies can take this into account when determining premiums by offering higher premiums to customers with a higher willingness to pay and cheaper offers to the others. When doing so, however, insurance companies will have to bear in mind that many people find the individualisation of prices according to the willingness to pay unfair.[15] This fact significantly limits the ability to price customers according to their willingness to pay, also in the insurance industry. From a purely economic point of view, however, aligning prices with the willingness to pay has positive effects, both for the insurance companies and their customers.

11 In economics, the individualisation of prices to absorb maximum willingness to pay is referred to as first-degree price discrimination or perfect price discrimination.[16] In insurance, this type of price discrimination has two main effects: On the one hand, all insurance policyholders can skim off their full willingness to pay, which allows the insurer to increase his turnover and maximise profit. On the other hand, the insurance can also be sold to customers whose willingness to pay is below the uniform price that would be chosen by the insurer if he could not or did not wish to discriminate against prices.[17] If it is assumed that people with a higher willingness to pay will not forego purchasing insurance despite higher individual premiums, price discrimination will also contribute to an expansion of insurance coverage in the population. The economic effect of the individualisation of insurance premiums is therefore positive.

C. Insurance Law

I. Preliminary Remarks

12 In Switzerland, the business of insurance is regulated by the Federal Constitution (FC)[18] and several federal acts. The insurance landscape is divided into two sectors: the social or public law sector and the private law sector. In the public law sector, there are ten social insurance branches that form the basis for social security;[19] mandatory health insurance is one of them. Mandatory health insurance is guided by the principle of solidarity of the insured persons[20] and its benefits are determined by statutory catalogue.[21] Anyone wishing to take out insurance cover in excess of benefits granted by the statutory catalogue must assume supplementary health insurance governed by private law. Swiss health insurances are conceived as individual insurance plans, in mandatory health insurance and in supplementary health insurance, as well as in all other types of private insurance.[22] Automobile insurance and insurance on contents are part of the private law sector. The supervision of mandatory health insurance is exercised by the Federal Office of Public Health,[23] whereas supervision

15 Empirical studies have shown, in particular, that price discrimination will often be regarded as unfair if it exceeds a certain level, is clearly disadvantageous compared to a reference price, or if other consumers pay significantly less; cf. Martin Fasnacht and Jochen Mahadevan, 'Grundlagen der Preisfairness – Bestandesaufnahme und Ansätze für zukünftige Forschung' (2010) 60 Journal für Betriebswirtschaft, 295, 302ff., with further references; Werner Reinartz and others, *Preisdifferenzierung und -dispersion im Handel*, (White Paper, 2017) <www.marketing.uni-koeln.de/sites/marketingarea/user_upload/171130_Whitepaper_Preisdifferenzierung_und_-dispersion_im_Handel.pdf> accessed 25 September 2018, 11; Florian Engelmaier and others, *Price Discrimination and Fairness Concerns*, Munich Discussion Paper No. 2012-7 (Ludwig-Maximillians-Universiät München 2012) <https://epub.ub.uni-muenchen.de/12735/1/Englmaier_Gratz_Reisinger-Price_Discrimination_and_Fairness_Concerns.pdf> accessed 3 June 2019; Simon Lee and Abdou Illia, 'Perceived price fairness of dynamic pricing' (2011) 111 Industrial Management & Data Systems 2011, 531; Kelly L. Haws and William O. Bearden, 'Dynamic Pricing and Consumer Fairness Perceptions' (2006) 33 Journal of Consumer Research 2006, 304; Matthew A. Edwards, 'Price and Prejudice: The Case against Consumer Equality in the Information Age' (2006) 10 Lewis & Clark L.Rev., 559.

16 Lars A. Stole, 'Price Discrimination and Competition', in: Mark Armstrong and Robert Porter (eds) *Handbook of Industrial Organization* (Elsevier 2007), 2221, 2224 ff.

17 Florent Thouvenin, 'Dynamische Preise' (2016) Jusletter IT dated 22. September 2016, para 5ff.

18 E.g. Art. 98 para 3 Federal Constitution (Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101) for private insurance or Art. 117 para 1 FC for health and accident insurance (Rolf H. Weber and Rainer Baisch, *Versicherungsaufsichtsrecht* (2nd edn, Stämpfli Verlag 2017), 41ff.).

19 Stephan Furrer, *Schweizerisches Privatversicherungsrecht* (Schulthess 2011) point 2.31.

20 Gertrud E. Bollier, *Leitfaden schweizerische Sozialversicherung*, vol I (15th edn, Kantonale Drucksachen- & Materialienzentrale 2018) 411.

21 Stefan Felder, 'Ökonomische Überlegungen zum Kontrahierungszwang in der Obligatorischen Krankenpflegeversicherung' (2018) 62 Schweizerische Zeitschrift für Sozialversicherung und berufliche Vorsorge, 95, 95.

22 Ueli Kieser, 'Art. 3 KVG' in: Ueli Kieser and others (eds) *KVG/UVG Kommentar: Bundesgesetze über die Krankenversicherung, die Unfallversicherung und den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) mit weiteren Erlassen* (Orell Füssli 2018) para 1.

23 Art. 56 in conjunction with Art. 34 of the Federal Act on the Supervision of Social Health Insurance

of private insurances pursuant to the Insurance Supervision Act (ISA)[24] is exercised by the Swiss Financial Market Supervisory Authority (FINMA).[25]

13 In contrast to Switzerland, the insurance business in the U.S. is primarily regulated on a state level. Besides some federal statutes for health insurance and some limited monitoring of insurance, there is no significant federal insurance regulation.[26] The insurance regulation primarily emanates from the courts, the state legislatures and the state regulatory agencies.[27] This is particularly true for automobile insurance and insurance on contents, which is called tenant or renters insurance.[28] The U.S. health insurance system differs from the Swiss system as it does not distinguish between mandatory and supplementary health insurance. The U.S. has no comprehensive national health insurance programme.[29] Rather there are three different types of health insurance: public health care coverage, employer-provided health insurance, and individually purchased or small group insurance. The public health care insurance programmes are Medicare and Medicaid. Approximately 55-60% of health insurance policies are employer-provided through group insurance policies.[30] Only a small portion of health insurances are taken out as individual policies.[31]

14 California's insurance laws are enforced by the Insurance Commissioner.[32] His functions and duties are exercised and performed by the California Department of Insurance (CDI).[33] Furthermore, the Commissioner has the statutory right to supplement the California Insurance Code (INS)[34] with rules and regulations. These administrative regulations are compiled in Chapter 5 of Title 10 of the California Code of Regulations (CCR), the codification of Californian administrative law.[35]

II. Switzerland

1. Mandatory Health Insurance

15 Mandatory health insurance in Switzerland is regulated by the Federal Health Insurance Act (HIA)[36] and the Ordinance on Health Insurance (OHI).[37] These laws are authoritative in determining whether health insurance premiums may be personalised. Neither the HIA nor the OHI address the personalisation of insurance contracts specifically. The premiums are determined by health insurers and not by an authority.[38] However, the principles governing the calculation of premiums for mandatory health insurance are set out in Art. 61ff. HIA and Art. 89ff. OHI. As a general rule and as far as the HIA does not provide for exceptions, health insurers have to charge the same premiums to all of their insured persons (unitary premium/premium per capita).[39] But an exhaustive list of criteria set forth by statute may be considered for adjusting the premiums to certain groups of insured and specific types of insurances. These criteria are place of residence,[40] age group (children, teenagers and adults),[41] limited

(Bundesgesetz betreffend die Aufsicht über die soziale Krankenversicherung vom 26. September 2014, SR 832.12).

24 Bundesgesetz betreffend die Aufsicht über Versicherungsunternehmen vom 17. Dezember 2004, SR 961.01.

25 Art. 46 ISA.

26 John F. Dobbyn and Christopher C. French, *Insurance Law in a nutshell* (5th edn, West Academic Publishing 2016) 501; Spencer Kook and Paul Rodriguez, 'Overview of California insurance law', in: Hinshaw & Culbertson LLP and Kristina Alexander (eds) *California Insurance Law & Practice* (Matthew Bender Inc. 2018) para 1.02[1], with further references. The Federal Insurance Office has the authority to monitor all aspects of the U.S. insurance industry (31 U.S.C. § 313).

27 Dobbyn and French (n 26) 501.

28 For the sake of simplicity, only the term "renters insurance" is used in this article.

29 Barry R. Furrow and others, *Health Law* (3rd edn, West Academic Publishing 2015) 400.

30 Dobbyn and French (n 26) 40 et. seq.; Statista, 'Distribution of U.S. population with health insurance 2011-2017, by coverage' <www.statista.com/statistics/235223/distribution-of-us-population-with-health-insurance-by-coverage/> accessed 25 March 2019.

31 The percentage of individually (direct) purchased health insurance policies increased from 9.8% in 2011 to 16% in 2017 (*ibid*).

32 INS §§ 12900 and 12921; B.E. Witkin, 'Chapter II. Insurance' in: *Summary of California Law* (11th edn, Witkin Legal Institute 2018) para 9(2); Kook and Rodriguez (n 26) para 1.08[1].

33 INS § 12906; Kook and Rodriguez (n 26) para 1.08[1].

34 Cf. California Legislative Information, <https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=INS&tocTitle=+Insurance+Code+-+INS>, accessed 1 May 2019.

35 Kook and Rodriguez (n 26) para 1.08[1]; Witkin (n 32) para 6(2).

36 Bundesgesetz über die Krankenversicherung vom 18. März 1994, SR 832.10.

37 Verordnung über die Krankenversicherung vom 27. Juni 1995, SR 832.102.

38 Ueli Kieser, 'Art. 61' in: Ueli Kieser and others (eds) *KVG/UVG Kommentar: Bundesgesetze über die Krankenversicherung, die Unfallversicherung und den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) mit weiteren Erlassen* (Orell Füssli 2018) para 1.

39 Art. 61 para 1 KVG. Kieser (n 38) para 3.

40 Art. 61 para 1, 2 and 2bis HIA.

41 Art. 61 para 3 and 3bis HIA.

choice of service providers,[42] choice of deductible[43] or bonus-related increases.[44] Accordingly, there is no leeway for insurance companies to personalise the premiums in mandatory health insurance.

2. Other Insurances

a.) Freedom of Contract

16 The question to what extent private insurers may individualise insurance contracts covering supplementary health benefits, automobile or renters insurance, is governed by the provisions of the Insurance Contract Act (ICA), the ISA and the associated Insurance Supervision Ordinance (ISO).[45] In private insurance law, the ICA supersedes the general provisions of the Code of Obligations (CO).[46]

17 There is no provision in these insurance statutes which would standardise or even prohibit the individualisation of insurance contracts. In addition, the relationship with the insured person is governed by the freedom of contract principle, meaning there is no general obligation for insurance companies to conclude a specific insurance contract, neither for mandatory, nor for voluntary insurance.[47]

18 However, mandatory law, public order and the right of personality set limits to freedom of contract in the area of private insurance.[48] Furthermore, insurance contracts with an impossible, illegal or immoral content are void. But, in general, the individualisation of insurance contracts is neither impossible, nor a violation of public order or morality. With regard to legality, certain compelling requirements for insurance contracts are set forth by Art. 97ff ICA.[49] However, these provisions do not contain rules on individualisation either.[50] Nevertheless, it is conceivable that individualisation of policies could lead to legally relevant discrimination against policyholders and hence would interfere with their right of personality. This question will be discussed in more detail below.[51]

b.) Protection against abusive behaviour

19 Even if private insurance law does not contain any specific provisions prohibiting the individualisation of insurance contracts - at least with regard to certain types of insurances - the insurers' freedom of contract is limited by ISA's provisions on the protection of the insured against abuse. The ISA's objective is not only to protect the insured against the risks stemming from insurance companies becoming insolvent, but also to protect them against abusive practices of insurance companies.[52] Accordingly, the protection against abuse is part of FINMA's mandate.[53] However, FINMA's respective supervisory competences differ for different types of insurance. While the legislator does not provide for a systematic preventive review of rates and conditions of most insurance contracts,[54] the rates as well as the general terms and conditions of occupational pension schemes and supplementary health benefits insurance have to be submitted to FINMA for prior approval.[55] For these two types of insurance, FINMA must grant the approval, if the proposed premiums do not jeopardise the solvency of the insurance company and do not lead to an abuse of the insured.[56]

42 Art. 62 para 1 HIA.

43 Art. 62 para 2 lit. a HIA, Art. 93ff. OHI.

44 Art. 62 para 2. lit. b HIA, Art. 96ff. OHI.

45 Bundesgesetz über den Versicherungsvertrag vom 2. April 1908, SR 221.229.1 and Verordnung über die Beaufsichtigung von privaten Versicherungsunternehmen vom 9. November 2005, SR 961.011.

46 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220; Art. 100 para 1 ICA; Hardy Landolt and Stephan Weber, *Privatversicherungsrecht in a nutshell* (Dike 2011) 20. If an aspect is not regulated by provisions of the ICA, the general provisions of the CO are applicable, as expressly stated in the ICA (Moritz W. Kuhn, *Privatversicherungsrecht* (Schulthess 2010) 98). Cf. on micro-segmentation and contractual norms: Weber (n 1) para 41.

47 Stephan Fuhrer, *Schweizerisches Privatversicherungsrecht* (Schulthess 2011) 66; Landolt and Weber (n 46) 38.

48 Art. 19 para 2 and Art. 20 para 1 CO; Kurt Pärli and others, 'Ungleiche Prämien aufgrund von Nationalität, Alter und Geschlecht in der Motorfahrzeugversicherung – ein Diskriminierungsproblem? (2019) Haftung und Versicherung, 16, 23; Lanz (n 8) 155; Bernhard Waldmann, 'Nationalitätsbedingte Erhöhung der Autoversicherungsprämien Kurzbegutachtung eines Einzelfalls von grundlegender Tragweite' (2007) Haftung und Versicherung, 65, 68.

49 See: Fuhrer (n 47) 42.

50 For further restrictions on freedom of contract in Swiss insurance law, see: Fuhrer (n 47) 99ff.

51 See below, D.

52 Art. 1 para 2 ISA. Rolf H. Weber, 'Big Data – Rechtliche Grenzen von unbegrenzten Möglichkeiten' in: Stephan Fuhrer (ed) *Jahrbuch Schweizerische Gesellschaft für Haftpflicht und Versicherung 2018* (Schulthess 2018), 87, 94.

53 Art. 46 para 1 lit. f ISA.

54 Monica Mächler, 'Art. 1 ISA' in: Peter Ch. Hsu and Eric Stupp (eds) *Basler Kommentar Versicherungsaufsichtsgesetz* (Helbing Lichtenhahn 2013) para 51; Weber (n 52) 87. On the occasion of the revision of the ISA in 2003, there was a change from a preventive to a subsequent control of insurance products, see: Swiss Federal Council, *Botschaft vom 9. Mai 2003 zu einem Gesetz betreffend die Aufsicht über Versicherungsunternehmen (Versicherungsaufsichtsgesetz, ISA) und zur Änderung des Bundesgesetzes über den Versicherungsvertrag* (BBl 2003) 3789, 3790ff. and 3798ff.

55 Art. 4 para 2 lit. r ISA.

56 Art. 38 ISA; Bernhard Rütsche, *Aufsicht im Bereich der Krankenzusatzversicherungen* (Schulthess 2017) point 20.

20 Other private insurances, such as automobile insurance or insurance on contents, are not subject to comparable rules. With regard to these types of insurances, the question whether FINMA may and must intervene depends on how the notion of "abuse" pursuant to Art. 1 ISA is construed.[57] While it is clear that FINMA has a statutory competence to protect the insured against abuse,[58] it is contested whether FINMA must take general action against abuses.[59] Narrower interpretations suggest that the overall aim of preventing abuse shall merely guide the interpretation and application of the provisions of ISA, but does not serve as a separate legal basis for intervention by FINMA.[60] If one follows this view, FINMA can merely intervene against the individualisation of rates requiring approval, i.e. the rates for occupational pension schemes and supplementary health benefits insurance.[61] According to a broader interpretation, an intervention to prevent abuse is generally possible. This is the view taken by the Swiss Federal Council, who specified the notion of abuse in Art. 117 ISO and inter alia qualified legally or actuarially unjustified substantial differentiations as abusive.[62] However, the effect of this provision is unclear as scholars rightly question the Federal Council's competence to enshrine such substantial obligations in an implementing ordinance such as the ISO.[63]

21 Even if one assumes, however, that FINMA is generally competent to take action against abuse with regard to all types of insurance, this does not preclude the individualisation of insurance contracts since varying conditions and premiums for individual customers cannot be qualified as abuse – at least as far as they are actuarially justified. This is probably always the case with individualisation according to the risk profile.[64] While an individualisation based on the willingness to pay cannot be justified from an actuarial point of view, the concept of abuse does not imply an obligation for equal treatment. As a consequence, this form of individualisation should also be permissible under Swiss insurance law, especially since it has positive economic effects.[65]

III. U.S./California

1. Health Insurance

22 In the U.S., health insurance is regulated on the federal level in the Patient Protection and Affordable Care Act (ACA)[66] and the Health Insurance Portability and Accountability Act (HIPAA).[67] On a Californian state level, all health insurance policies marketed, issued or delivered to a California resident are subject to the provisions of the California Insurance Code (INS).[68] The California Department of Insurance is responsible for regulating all entities engaged in the business of health insurance, with the exception of managed care plans.[69] Such managed care plans are subject to the regulatory jurisdiction of the Department of Managed Health Care (DMHC).[70]

57 Cf. Rütsche (n 56) point 62; Weber and Baisch (n 18) 143; Shelby du Pasquier and Valérie Menoud 'Art. 46 ISA' in: Peter Ch. Hsu and Eric Stupp (eds) *Basler Kommentar Versicherungsaufsichtsgesetz* (Helbing Lichtenhahn 2013) para 13.

58 Art. 1 para 2 ISA and Art. 46 para 1 lit. f ISA.

59 Cf. Hubert Stöckli, 'Totalrevision VVG: Probebohrungen im Entwurf des Bundesrates' (2012) Schweizerische Juristen-Zeitung, 505, 513; Fuhrer (n 47) 556; as well as du Pasquier and Menoud (n 57) para 13, 33, 37; without restrictions to Art. 46 para 1 (f) ISA: Weber and Baisch (n 18) 210; Waldmann (n 48) 65 and 75, also assumes that pursuant to Art. 46 para 1 lit. f ISA and Art. 117 para 2 ISO as well as of Art. 5 Abs. 3 FC FINMA must prevent discrimination.

60 Weber (n 52) 94. Cf. also Weber and Baisch (n 18) 44; Mächler (n 54) 53.

61 Art. 33 para 3 and Art. 38 ISA.

62 Art. 117 para 2 ISO.

63 For a discussion of this controversy cf. Florent Thouvenin, 'Privatversicherungen: Datenschutzrecht als Grenze der Individualisierung?', in: Astrid Epiney and Déborah Sangsue (eds) *Datenschutz und Gesundheitsrecht/Protection des données et droit de la santé* (Schulthess 2019), 15, 23; Weber (Fn. 52) 95.

64 See above, B.I.

65 See above, B.II.

66 Patient Protection and Affordable Care Act of 2010, 42 U.S.C., § 18001.

67 Health Insurance Portability and Accountability Act of 1996, 26 U.S.C., § 9801. Notably, employer-provided health insurance coverage may also be subject to ERISA (Employee Retirement Income Security Act of 1974, 29 U.S.C. §§ 1001 to 1461 [1974], which imposes various requirements considering participation, funding, vesting and enforcement of rights under employee benefit plans (cf. Justice H. Walter Croskey and others, 'Chapter 6: First Party Coverages', *California Practice Guide: Insurance Litigation* (The Rutter Group 2017) para 1420ff.).

68 Witkin (n 32) para 169.

69 Managed care plans do not qualify as insurance companies and they are not regulated by the INS or administrative regulations issued under it (Witkin (n 32) para 170). Managed care plans, in California characterised as health care service plans (Cal. Health & Saf.C. § 1345(f)), ensure the provision and payment of health services to its members through contracts with health care providers (e.g. doctors, hospitals, etc.). Different types of managed care contracts, like full-service managed care plans (i.e. Health Maintenance Organizations (HMOs)), Medi-Cal managed care plans, Medicare Advantage plans, Preferred Provider Organizations (PPOs) and Point of Service (POS) plans are offered by managed care plans (cf. Witkin (n 32) para 170); Croskey and others (n 67) para 900.

70 Croskey and others (n 67) para 700.5ff.

a.) Public health care coverage: Medicare & Medicaid

23 Medicare[71] is a mandatory health insurance programme for people over the age of 65 or for people with certain disabilities or an end-stage kidney disease.[72] It consists of four programmes, parts A (hospital insurance),[73] B (voluntary supplemental medical insurance),[74] C (private-sector alternative to Parts A and B),[75] and D (outpatient prescription drugs),[76] Medicare is administered by the Center on Medicare and Medicaid Services (CMS), which is part of the U.S. Department of Health and Human Services (HHS).[77]

24 Since Medicare is mostly funded by taxes on wages paid over lifetime,[78] most people in the U.S. don't pay a Part A premium when they enter retirement. The Premiums for all Medicare parts are determined[79] and depend on given factors like income, receipt of social security benefits or the Medicare part chosen (Part B, C or D).[80] Therefore, an individualisation of these health insurance "contracts" is not possible.

25 Anyone enrolled in Medicare can purchase a privately offered Medicare supplement insurance (also called Medigap), which is sold as group or individual policy.[81] The insured pay a monthly premium for Medigap[82] and policies may only be designed in accordance with model forms approved by the National Association of Insurance Commissioners.[83] In California, Medigap policies have to be approved by the Commissioner[84] and the premiums shall be calculated in accordance with accepted actuarial principles and practices.[85] Pricing can be based on the actual age (age-rated premium), the age at the time the Medigap policy was taken out (issue age-rated premium), or may be the same for everyone living in a given territory (community rated premium).[86]

26 Medicaid[87] is an insurance programme for people who do not have the financial means to pay for health insurance themselves, aged or blind people in need of long-term care services, and disabled persons with low incomes.[88] In California, the California Department of Health Services (DHS) is in charge of the administration of Medicaid (called Medi-Cal). As with Medicare, there is no leeway regarding the individualisation of Medicaid health insurance premiums: Eligible Californians receive Medicare respectively Medi-Cal as a benefit without paying a premium[89] and the health benefits are determined by federal and state regulation.[90]

b.) Employer-provided coverage (group health insurance)

27 The most common way to get health insurance in the U.S. is through a group plan for employees.[91] Employers with more than 50 employees (large employers) are encouraged by the federal government to provide health insurance with minimum essential coverage.[92] This so-called "employer-provided coverage" is usually purchased by the employer from an insurance company. Some large employers "self-insure" their employees.[93] However, even self-insuring employers often (have

71 42 U.S.C. § 1395-1395kkk-1; 42 C.F.R. Parts 405-426 and 482-498; see Furrow and others (n 29) 403.

72 Dobbyn and French (n 26) 42ff; Robert H. Jerry and Douglas R. Richmond, *Understanding Insurance Law* (6th edn, LexisNexis 2018) 420.

73 Dobbyn and French (n 26) 43; U.S. Government, 'What Medicare Covers' <www.medicare.gov/what-medicare-covers/what-part-a-covers> accessed 4 June 2019.

74 Furrow and others (n 29) 401.

75 So called "Medicare Advantage". Tom Baker and Kyle D. Logue, *Insurance Law and Policy: Cases, Materials and Problems* (4th edn, Wolters Kluwer 2017) 259.

76 Furrow and others (n 29) 401 et seq.

77 Furrow and others (n 29) 403.

78 Dobbyn and French (n 26) 43.

79 See U.S. Government, 'Medicare costs at a glance' <www.medicare.gov/your-medicare-costs/costs-at-a-glance/costs-at-glance.html>, accessed 4 June 2019.

80 See Harvey L. McCormick, *Medicare and Medicaid Claims and Procedures* (4th edn, Thomson West 2017) para 1:65.

81 INS § 10192.4(m); 10 CCR § 2220.51.

82 U.S. Government, 'What's Medicare Supplement Insurance (Medigap)?' <www.medicare.gov/supplements-other-insurance/whats-medicare-supplement-insurance-medigap> accessed 12 June 2019.

83 42 U.S.C. § 1395ss(p); Croskey and others (n 67) para 745.

84 INS §§ 10192.1 in connection with 10291.5, 10192.14(c) and 10191.15(c).

85 INS § 10192.14(a)(B).

86 U.S. Government, 'Costs of Medigap policies' <www.medicare.gov/supplements-other-insurance/whats-medicare-supplement-insurance-medigap/medigap-costs/costs-of-medigap-policies>, accessed 4 June 2019.

87 Medicaid is codified in 42 U.S.C. §§ 1396 a-f; cf. McCormick (n 80) para 22:16.

88 Dobbyn and French (n 26) 44; Jerry and Richmond (n 72) 420.

89 California Department of Insurance, 'Overview: Healthcare Coverage in California' <www.insurance.ca.gov/01-consumers/110-health/10-basics/overview.cfm> accessed 25 March 2019.

90 See Furrow and others (n 29) 478ff.

91 Dobbyn and French (n 26) 40; see also: 42 U.S.C. § 300gg-91.

92 Dobbyn and French (n 26) 41.

93 To self-insuring employers a different set of rules applies than to insurance policies or health plans, (California Department of Insurance, 'Group (Employer-Based) Health Coverage' <www.insurance.ca.gov/01-consumers/110-health/10-basics/overview.cfm> accessed 12 June 2019.). Due to the length of this article, we decided not to take a closer look at these provisions for self-insuring employers.

to) use a health insurer to administer the programme and manage the health benefits.[94] Employer-provided health insurance is predominantly taken out as a group policy. Group policies are usually underwritten on the basis of factors common to the group as a whole, such as type of job, average age, etc.[95]

28 Within the scope of the ACA, all products that are approved for sale in the group health insurance market must be offered to any individual or employer in the state, and the health insurer must accept any individual or employer that applies for any of those products (guaranteed availability of coverage).[96] In California, group health insurance must be offered to all the employees of an employer.[97] All group health insurance policies must be approved by the Commissioner before they are issued or delivered to any person in California.[98] The approval of the Commissioner shall among others, prevent fraud, unfair trade practices, and economically unsound insurances.[99] A group health insurance policy shall also not be approved if it contains any provision which is unintelligible, uncertain, ambiguous, or abstruse, or likely to mislead a person to whom the policy is offered, delivered or issued, or if it fails to conform in any respect with any law of California.[100]

29 The framework of employer-provided coverage is set out in the master policy. The insurance company is bound by this master policy and can only include the factors specified therein in the risk assessment of an individual employee. Thus, the leeway for individualisation of policies will be very limited for the group health insurance.

c.) Individual and small group market

30 People who are not covered by one of the aforementioned governmental programmes or by their employer, can get health insurance from a private insurer on the individual or small group market.[101] On the individual market, individuals take out the insurance policy themselves, while the small group market provides group health plans maintained by a small employer.[102] The policy of an individually-purchased insurance is based on the buyer's risk profile and the premium is equal to the price the insurer deems adequate to insure said risk.[103]

31 Under the ACA, insurance premiums shall be "fair". As a result, the rating factors for health insurance policies on the individual or small group market are community rated and subject to limited adjustments based on age, geographic area, individual or family unit, and tobacco use.[104] Insurers must maintain a state-wide risk pool for both the individual market and the small group market[105] and are required to set an index rate for each pool for establishing the premium rates. The premium rates for individual and small group health insurance policies may only vary to a limited extent from the index rates.[106] Also the health insurance policies for the individual market and the respective premium rates have to be filed with and approved by the Commissioner before they are issued or delivered to any person in California.[107]

94 Dobbyn and French (n 26) 41; California Department of Insurance (n 93).

95 Croskey and others (n 67) para 1306.

96 45 CFR § 147.104.

97 Group health insurance is regulated in INS §§ 10270-10400; Michael A.S. Newman and others, 'Group life and Disability Insurance' in: Kristina Alexander and Hinshaw & Culbertson (eds) *California Insurance Law & Practice* (Matthew Bender 2018) vol 3, para 30.30 and 30.31[1].

98 INS §§ 10270.9 and 10290; Richard B. Hopkins, 'The Health and Disability Insurance Contract' in: Kristina Alexander and Hinshaw & Culbertson (eds) *California Insurance Law & Practice*, vol 2 (Matthew Bender 2018) para 26.11; *Ellena v. Department of Ins.*, 230 Cal. App. 4th 198 [2014].

99 INS § 10291.5(a)(1).

100 INS § 10270.95 in connection with INS § 10291.5(b)(1) & (13).

101 See: Dobbyn and French (n 26) 41ff; see INS § 10753 (q) (1) for the definition of a small employer in California with regard to insurance. See also: 42 U.S.C. § 300gg-91.

102 US.legal.com, 'Small Group Market (Health Care)' <https://definitions.uslegal.com/s/small-group-market-health-care/> accessed 25 March 2019; see: INS § 10753 (q) (1) for the definition of a small employer in California with regard to insurance. See also: 42 U.S.C. § 300gg-91.

103 James C. Castle and Paul Rodriguez, 'The Insurance Contract' in: Kristina Alexander and Hinshaw & Culbertson (eds) *California Insurance Law & Practice*, vol 2 (Matthew Bender 2018) para 8.02[4].

104 42 U.S.C. § 300gg(a)(1)(A); 45 CFR § 147.102; Timothy Stoltzfus Jost, Special Report, 'The Patient Protection and Affordable Care Act and the Health Care and Education Reconciliation Act of 2010' in: Kristina Alexander and Hinshaw & Culbertson (eds) *California Insurance Law & Practice* (Matthew Bender 2018) vol 2, II[B]. In terms of age, the rate shall not vary by more than 3 to 1 for adults (42 U.S.C. § 300gg(a)(1)(A)(iii)). The rating factor for tobacco use shall not vary by more than 1.5 to 1 (42 U.S.C. § 300gg(a)(1)(A)(iv)). California, however, has prohibited the use of the rating factor for tobacco use for insurance policies on the individual or small group market (INS § 10753.14(b) for small group policies and INS § 10965.9(b) for individually purchased policies). See also: John K. DiMugno and Paul E.B. Glad, *California Insurance Law Handbook* (April 2018 Update, Thomson West) para 37A:3; 42 U.S.C. § 300gg(a)(2)(A).

105 42 U.S.C. § 18032(c). Adam M. Cole, 'Legal Opinion Pursuant to Insurance Code Section 12921.9 Regarding Premium Cross-Subsidization Across Market Segments in Health Insurance' (California Department of Insurance, 13 June, 2014) <www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/opinions.cfm>, 2.

106 INS §§ 10965.3(h)(2 et seq.), 10753.05(k)(2 et seq.), quod vide: 45 CFR § 156.80(d)(2)); Adam M. Cole (n 105).

107 INS § 10290; Hopkins (n 98) para 26.11.

The INS contains a long list of circumstances under which the Commissioner shall not approve health insurance policies.[108] Should the Commissioner find that the benefits provided under the policy are unreasonable in relation to the premium charged, he may withdraw an individual or mass-marketed policy's approval.[109]

32 As with group insurance, the ACA requires that all products that are approved for sale in the individual or small group market must be offered to any individual or employer in the state, and the health insurer must accept any individual or employer that applies for any of those products (guaranteed availability of coverage).[110] Also California has enacted a detailed review process for rates increases when implementing the respective provisions of the ACA.[111] If the CDI determines that a rate is unreasonable or not justified, the insurer shall notify the policyholder of this determination.[112] However, the Commissioner's authority is limited to requesting rate changes; he cannot deny or approve proposed rate changes.[113]

33 The leeway for individualisation of individually purchased health insurance or small group health insurance is very limited. Especially since individual policies have to be based on one risk pool and the rates may only be adjusted with regard to geographic region, size of family, and age. The premiums also have to be based on the approved index rate, which will hinder individualisation. The requirements of the ACA, such as the guaranteed availability and renewability of coverage, are another obstacle for individualising insurance rates. Nevertheless, the requirements in connection with unreasonable rate increases do not reduce the leeway for individualisation, at least in those cases in which individualisation is based on the risk profile. Individualisation on the basis of risk will probably not be deemed "unreasonable" as long as it is actuarially sound. In the case of individualisation based on the willingness to pay, however, the requirement to inform customers about unreasonable rate increases could hinder such individualisation, provided that the criterion of the willingness to pay would meet the "unreasonable" threshold. Affected people could regard this practice as unfair and might switch insurers upon receiving a respective-notice.

108 See INS § 10291.5(b).

109 INS § 10293 (a), see also: 10 CCR § 2222.10-19. See John A. Gebauer and others, 'Insurance Contracts and Coverage', *California Jurisprudence 3d* (February 2019 Update) para 272.

110 45 CFR § 147.104.

111 42 U.S.C. § 300gg–94; 45 CFR § 154.200 - 45 CFR § 154.230; INS §§ 10181 - 10181.13.

112 INS §§ 10181.3(g) and 10199.1(d).

113 INS § 10181.3.

2. Property Insurance

a.) Preliminary remarks

34 Since the business of insurance in the U.S. is primarily regulated on a state level, there are no federal regulations on property-casualty insurance.[114] On a Californian state level, most insurance on risk and operations are regulated in Proposition 103, an amendment of the Insurance Code adopted in 1988.[115] Proposition 103 shall, among others, protect consumers from arbitrary insurance rates and practices. For all Californians, insurance must be fair, available, and affordable.[116] No rate which is excessive, inadequate or unfairly discriminatory shall be approved or remain in effect.[117] By enacting Proposition 103 California has become a prior-approval state and like most insurance on risk and operations, property-casualty insurances like homeowners, renters and automobile insurance are covered by Proposition 103.[118] Thus, all property and casualty insurance rates have to be approved by California's Insurance Commissioner prior to use.[119]

35 In February 2015 the Commissioner has prohibited price optimisation in his "Notice Regarding Unfair Discrimination in Rating: Prize Optimization". Prize optimisation is therein defined 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 Commissioner qualifies any form of price optimisation in the ratemaking process as unfairly discriminatory and as a violation of Californian law. This assessment is based on the finding that "*Price Optimization does not seek to arrive at an actuarially sound estimate of the risk of loss and other future costs of a risk transfer.*"[120] Accordingly, there is no leeway for the personalisation of property and casualty insurance contracts based on an insured's willingness to pay.

114 The business of insurance is almost exclusively regulated by the states, see: Baker and Logue (n 75) 631ff; Dobbyn and French (n 26) 501ff.

115 Article 10, Reduction and Control of Insurance Rates, INS §§ 1861.01-1861.16. Witkin (n 32) para 11 (1).

116 Witkin (n 32) para 11(1); Richard G. De La Mora and Spencer Y. Kook, 'Property-Casualty Insurance Ratemaking and Rate Regulation' in: Hinshaw & Culbertson LLP and Kristina Alexander (eds) *California Insurance Law & Practice* (Matthew Bender Inc. 2018) para 6A.03.

117 INS § 1861.05(a).

118 Kook and Rodriguez (n 26) para 1.08[3].

119 INS § 1861.01(c); Kook and Rodriguez (n 26) para 1.03, [3] and para 1.07[3].

120 California Insurance Commissioner, *Notice regarding unfair discrimination in rating: price optimization* (Department of Insurance, State of California February 18, 2015) <www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/upload/PriceOptimization.pdf>.

b.) Renters Insurance

36 Renters insurance in California usually consists of different insurance coverages like personal property or liability insurance. In this paper we only analyse the regulation concerning the insurance of personal property.

37 Neither Proposition 103, nor the INS contains specific requirements regarding property insurance and hence the general rules set forth by Proposition 103 apply. Renters insurance premiums may not be excessive, inadequate or unfairly discriminatory.[121] Premiums are deemed excessive if it is expected that the insurance company will generate an excessive profit[122] and they are considered inadequate if they are expected to prevent an efficient insurance company from generating an adequate return.[123] To investigate whether an insurance rate is excessive or inadequate, the Commissioner has to balance the interest of the insured in favourable prices with the insurance companies' interest in high earnings. He also has to take into account that certain insurance policies are in the general public's interest or legally prescribed.[124] A so-called "ratemaking formula" is used to distinguish appropriate from inadequate or excessive rates. The formula must be applied by all insurers and sets forth the maximum[125] and minimum[126] permitted earned premium. Rates within this range can be described as "fair and reasonable" and "constitutional".[127] Nevertheless, the Commissioner still may assess on a case-by-case basis whether a rate is "unfairly discriminatory". Notably, there are no rules and regulations specifying how this assessment shall be made in connection with property-casualty insurance.[128]

c.) Automobile Insurance

38 The aforementioned system of pre-approval of insurance rates also applies to automobile insurance. In addition, Proposition 103 has set forth additional requirements for automobile insurance.[129] The permitted rate-making factors are determined and given a hierarchy in INS § 1861.02(a). These are in decreasing order of importance: (1) the insured's driving safety record; (2) the number of miles driven annually; (3) the years of driving experience; and (4) other factors that have a substantial relationship to the risk of loss and that were set forth in a regulation adopted by the Commissioner. The Commissioner has specified sixteen such optional rating factors.[130] Insurers can base their premiums on these factors as well. However, these optional rating factors must not be weighted greater than the weight of the third mandatory factor, i.e. the years of driving experience.[131] The use of rating factors not set forth in the CCR is prohibited.[132] Considering any other criteria without approval would constitute unfair discrimination.[133]

39 While insurers can take the insured's driving safety record into account, this does not mean that they may use crash recorder data for ratemaking, since the law sets forth clear limits with regard to what data may be used in rate-making.[134] Insurers may consider the amount of annually driven miles, but usually base this factor on an own estimation or an estimation by the policyholder. While insurers are free to offer rates that are based on verified actual mileage rather than estimated mileage, participation in these actual mileage programmes is purely voluntary.[135]

121 INS § 1861.05(a).

122 10 CCR § 2642.1.

123 10 CCR § 2642.3.

124 See: 10 CCR § 2642.1; 10 CCR § 2642.3.

125 10 CCR § 2644.2.

126 10 CCR § 2644.3.

127 Cf. De La Mora and Kook (n 116) para 6A.03 and [8][f]ff; The California Supreme Court endorsed the formula, cf. *20th Century Ins. Co. v. Garamendi,* 8 Cal. 4th 216 [1994].

128 De La Mora and Kook (n 116) para 6A.04(2). But compare D.III. with regard to anti-discrimination laws.

129 De La Mora and Kook (n 116) para 6A.04, [5][a].

130 According to 10 CCR § 2632.5(d)(l)-(16) these are: type of vehicle; vehicle performance capabilities, including alterations made subsequent to original manufacture; type of use of vehicle (pleasure only, commute, business, farm, commute mileage, etc.); percentage use of the vehicle by the rated driver; multi-vehicle households; academic standing of the rated driver; completion of driver training or defensive driving courses by the rated driver; vehicle characteristics, including engine size, safety and protective devices, damageability, reparability, and theft deterrent devices; gender of the rated driver; marital status of the rated driver; persistency (only for renewal of policy, see *California Insurance Law Dictionary and Desk Reference* (2018 edn, Thomson West) para P36.5); non-smoker; secondary driver characteristics; multi-policies with the same, or an affiliated, company; relative claims frequency or relative claims severity.

131 De La Mora and Kook (n 116) para 6A.04, [5][c]; cf. *Spanish Speaking Citizens' Foundation, Inc. v. Low*, 85 Cal.App.4th 1179 [2000], 1221.

132 10 CCR § 2632.4(a).

133 INS § § 1861.02(a)(4)

134 For example, public records on convictions may be considered. Cf. 10 CCR § 2632.5(c)(1)). De La Mora and Kook (n 116) para 6A.04, [5][c].

135 (10 CCR § 2632.5(c)(2)(E) & (F)). De La Mora and Kook (n 116) para 6A.04, [5][c].

IV. Findings

40 While Switzerland and the U.S./California apply a very different approach for providing health care insurance, both jurisdictions align with regard to the limited leeway for the individualisation of health insurance contracts. In Switzerland, the individualisation of mandatory health insurance is not allowed, while there is quite some leeway for the individualisation of supplementary health insurance if such individualisation does not qualify as an abuse. In the U.S./California, there is almost no leeway for the individualisation of insurance contracts in the health insurance market as this market is comprehensively regulated and leaves insurance companies with vanishingly little possibilities with regard to adjusting premiums on an individual level.

41 The regulatory approach in Switzerland and the U.S./California differs even more in other insurance markets, namely for automobile insurance and insurance on contents: In Switzerland, these types of insurance are based on the principle of freedom of contract. Therefore, insurance law does not limit the ability of insurance companies to individualise insurance contracts. One could be of a somewhat different opinion if it is assumed that FINMA is generally competent to take action against abuse and if it is argued that the individualisation of insurance contracts is to be qualified as an abuse. In our view, however, individual conditions and premiums cannot be qualified as abuse if they are actuarially justified, which should always be the case if the individualisation is based on the insured's risk profile. In addition, the notion of abuse does not imply an obligation of equal treatment. Accordingly, the individualisation of insurance contracts should also be permissible under Swiss insurance law if it is based on the insureds' willingness to pay.

42 In California, automobile and renters insurance are densely regulated and the rates are subject to prior approval by the California's Insurance Commissioner. While this approach limits the flexibility of insurance companies considerably, it does not exclude the personalisation of insurance contracts per se. Rather, the degree of permitted individualisation depends on the concrete specifications according to which the insurance premiums must be determined and how adjustable-rates are approved by the Commissioner. In our opinion, a personalised insurance contract cannot be deemed excessive, inadequate or unfairly discriminatory as a premium which is specifically adjusted to the risk of an individual person can hardly be deemed excessive or inappropriate. This should particularly hold true for premiums that comply with accepted actuarial standards. However, the margin for individualisation appears fairly limited as the maximum and minimum permitted premium is determined by law. In addition, the personalisation of renters or automobile insurance based on the insured's willingness to pay is straightforwardly prohibited in California. As a consequence, insurance companies in California have hardly any leeway to individualise insurance contracts.

D. Anti-discrimination Law

I. Preliminary Remarks

43 The personalisation of insurance contracts leads to people paying different premiums. This creates tensions with the constitutional principle of equal treatment, according to which individuals are to be treated equally as far as they possess equal characteristics. The equal treatment principle, however, does not prohibit all forms of differentiation and does not require unequal individuals to be treated equally. Yet, discriminating against certain protected characteristics is prohibited by the Swiss and the U.S. constitution. Thus, anti-discrimination law encompasses the question to what extent private parties are bound by the constitution. But anti-discrimination law is also found on a statutory level. In Switzerland, several specific statutes, as well as the general right to protection of personality enshrined in the Civil Code, need to be observed. Californian insurers are also subject to a variety of anti-discrimination laws on both the federal and the state level. The individualisation of insurance contracts thus has to navigate the conflicted interplay between contractual freedom and statutory limitations to discrimination. When doing so, distinguishing between different types of insurances, as well as understanding the rationales for rate adjustment, is of utmost importance.[136]

II. Switzerland

1. Federal Constitution

44 The Federal Constitution's non-discrimination principle determines that no-one may be discriminated against on the grounds of origin, race, sex, age, language, social position, way of life, religious, ideological or political conviction, or on the grounds of physical, mental or psychological disability (so-called "protected characteristics").[137] The primary addressee is the state,[138] but the

136 Cf. Bitter and Uphues (n 2) 148ff.

137 Art. 8 para 2 FC.

138 Giovanni Biaggini, 'Art. 8 BV' in: Giovani Biaggini (ed) *Bundesverfassung der Schweizerischen Eidgenossenschaft:*

non-discrimination principle is also binding on private individuals performing public functions,[139] such as insurance companies offering mandatory health insurance.[140] When offering such insurance, insurance companies may not take protected characteristics into account when exercising their actuarial discretion within the limits set by health insurance law.[141]

45 In contrast, the providers of private insurances, such as supplementary health, automobile or renters insurance are not directly bound by the constitutional non-discrimination principle.[142] Nevertheless, the constitution requires authorities to ensure that fundamental rights also become effective among private individuals, to the extent that the fundamental right in question is suitable for such "horizontal" application.[143] This also applies to FINMA, the authority supervising the insurance sector. Thus, FINMA must take account of the prohibition of discrimination in the application of the laws regulating the insurance sector, particularly when interpreting legal terms.[144]

46 For the individualisation of insurance contracts, this assessment could be relevant when construing and applying the concept of "abuse" in the ISA. If one follows the view that neither the ISA's objective[145] nor FINMA's statutory competences[146] serve as a basis for intervention by the supervisory authority,[147] the question of giving effect to the non-discrimination principle between private individuals arises only when examining the rates that are subject to approval; i.e. the rates for occupational pensions and supplementary health insurance.[148] Here, FINMA must take due account of the prohibition of discrimination when interpreting the concept of abuse.

47 At least in this area,[149] FINMA is mandated to intervene if an insurance company were to individualise the conditions based on a protected characteristic since such discrimination could be qualified as an abuse.[150] This applies to direct as well as indirect discrimination. As opposed to direct discrimination, which is taking place if an insurer discriminates the conditions of an insurance contract based on a protected characteristic, indirect discrimination takes place when the insurer does not account for a protected characteristic in its individualisation process, but the actual effects of individualisation would be particularly disadvantageous for people possessing a protected characteristic.[151] However, the existence of discrimination always requires the existence of a qualified unequal treatment of a protected group of persons. According to prevailing case law, this requires that the distinguishing feature being used as discriminant constitutes an essential element of the identity of the person concerned and is impossible or very difficult to give up.[152] Further, using a protected characteristic as discriminant can be justified if three conditions are met:[153] first, there must be an objective reason for the differentiation; second, it must pursue a legitimate aim; and third, the differential treatment needs to be proportionate to that aim.[154] As insurance companies will base the individualisation on objective reasons such as an insured's risk profile or willingness to pay while pursuing the legitimate aim of attracting additional customers, increasing their turnover, and fighting adverse selection and moral hazard, it is likely that the individualisation based on protected characteristics will be justified on a regular basis and is therefore not to be considered as an abuse in the sense of the ISA.

Kommentar (Orell Füssli 2017) para 18.

139 Art. 35 para 2 FC.

140 See: Swiss Federal Court (unpublished case no 5P.97/2006) [2006] at 3.3.

141 See above, C.II.1.

142 See Swiss Federal Court (BGE 129 III 35) [2003] at 5.2; critical Kurt Pärli,'Urteil des Bundesgerichts 5P.97/2006 vom 1. Juni 2006' (2007) Haftung und Versicherung, 46, 48 ff.; cf. below, D.II.4, on the protection against discrimination derived from the right to respect one's personality.

143 Art. 35 para 3 FC.

144 Advocating an interpretation in the light of fundamental rights: Jörg Paul Müller, *Verwirklichung der Grundrechte nach Art. 35 BV* (Stämpfli Verlag 2018) 103 ff.

145 Art. 1 ISA.

146 Art. 46 ISA.

147 See above, C.II.2.b).

148 Art. 4 para 2 lit. r in conjunction with Art. 38 ISA.

149 A more extensive interpretation of FINMA's mandate has been proposed, see above, C.II.2.b).

150 Same opinion Waldmann (n 48) 69.

151 Swiss Federal Court (BGE 139 I 169) [2013] at 7.2.1ff.; Swiss Federal Court (BGE 129 I 217) [2003] at 2.1; Biaggini (n 138) para 20, with further references; Rainer J. Schweizer 'Art. 8 BV in: Bernhard Ehrenzeller and others (eds) *Die Schweizerische Bundesverfassung: St. Galler Kommentar* (Dike and Schulthess 2014) para 51, with further references.

152 Swiss Federal Court (BGE 141 I 241) [2015] at 4.3.2; Swiss Federal Court (BGE 139 I 169) [2013] at 8.2.1; Swiss Federal Court (BGE 135 I 49) [2009] at 4.1; Swiss Fedral Court (BGE 134 I 49) [2008] at 3.1; Swiss Federal Court (BGE 126 II 377) [2000] at 6.

153 Biaggini (n 138) para 22; Schweizer (n 151) para 48; Swiss Federal Court (BGE 141 I 241) [2015] at 4.3.2; Swiss Federal Court (BGE 139 I 169) [2013] at 8.2.2.

154 Biaggini (n 138) para 26; Schweizer (n 151) para 54, with further references. However, the requirements for justification are not identical for all protected characteristics and there is no room for justification at all for certain characteristics, see: Biaggini (n 138) para 25; Schweizer (n 151) para 48.

2. Federal Act on the Elimination of Disadvantages of Persons with Disabilities (EDPD)

48 The Federal Act on the Elimination of Disadvantages for Persons with Disabilities (EDPD)[155] intends to prevent, reduce or eliminate disadvantages to which people with disabilities are exposed.[156] With this aim in mind, private individuals offering services to the public must not discriminate against disabled people on the basis of their disability.[157] This also applies to private insurances.[158] Discrimination occurs when people with disabilities are treated in a radically different and disadvantageous way, with the aim or the consequence of degrading them or excluding them from services.[159] However, the EDPD does not oblige private individuals to take certain (positive) measures to eliminate actual disadvantages, or to refrain from differentiating between customers.[160] In the event of discrimination, only compensation of no more than CHF 5'000 can be claimed.[161] The Act does not confer the right to conclude a contract.[162]

49 These requirements hardly impose any restrictions on the individualisation of insurance contracts. First of all, the legislator has made it clear that the law merely aims at preventing particularly unacceptable behaviour by private individuals lacking any tolerance that members of the society owe to each other.[163] Insurance companies do not exclude people with disabilities because of their disability, but because their disability represents a financial risk. Differentiating according to this risk is objectively justifiable.[164] It is therefore only questionable whether exclusion or degradation could be an (indirect) consequence of individualisation. The risk of exclusion cannot be ruled out, at least in the event of refusal to offer supplementary insurance. However, the access to health care as such is not at stake, as insurance companies are prohibited from excluding disabled people from mandatory health insurance. As the threshold has been set very high (particularly unacceptable behaviour), the refusal to offer supplementary insurance will hardly meet the requirements of the EDPD.

3. Federal Act on Human Genetic Testing (HGTA)

50 Insurers could use genetic tests for individualised risk-assessments and discriminate against individuals based on the conclusions that can be drawn from the results of genetic tests. However, the use of genetic information is constitutionally prohibited unless authorised by consent or law.[165] The Federal Act on Human Genetic Testing (HGTA) sets forth conditions under which human genetic testing may be performed in the context of insurance.[166] First and above all, insurance providers are prohibited from requiring pre-symptomatic or pre-natal genetic tests prior to providing insurance.[167] For certain types of insurance, such as mandatory health insurance, supplementary health insurance, and insurance for illness and maternity leave, the prohibition on utilising or requesting genetic tests is absolute.[168] For other types of insurance, the insurance provider may require applicants to disclose previously taken pre-symptomatic genetic tests if these tests provide reliable results and are of demonstrable scientific value from a technical and a medical practice perspective.[169]

51 These provisions shall balance the interests between persons seeking out insurance and the insurance companies' interest in comprehensive information on the insured.[170] However, the prohibition merely covers the utilisation of pre-symptomatic and pre-natal genetic tests. Information obtained from genetic testing for diagnosis is not covered. Nevertheless, the HGTA stipulates that, in general, no one shall be discriminated against on the basis of genetic information.[171]

155 Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen vom 13. Dezember 2002, SR 151.3.

156 Art. 1 para 1 EDPD.

157 Art. 6 EDPD.

158 Similar opinion: Pärli (n 142) 50; Swiss Federal Court (unpublished case no 5P.97/2006) [2006] at 4.2, in the case of supplementary health insurance.

159 Art. 2 lit. d Federal Ordinance on the Elimination of Disadvantages for Persons with Disabilities (Verordnung über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen vom 19. November 2003, SR 151.31).

160 Swiss Federal Council, *Botschaft vom 11. Dezember 2000 zur Volksinitiative «Gleiche Rechte für Behinderte» und zum Entwurf eines Bundesgesetzes über die Beseitigung von Benachteiligungen behinderter Menschen* (BBl 2001) 1715, 1780; see Swiss Federal Court (unpublished case no 5P.97/2006) [2006] at 4.1.

161 Art. 8 para 3 in conjunction with Art. 11 para 2 EDPD.

162 Swiss Federal Court (unpublished case no 5P.97/2006) [2006] at 4.1.

163 Swiss Federal Council (n 160) 1780.

164 Same opinon: Pärli (n 142) 51.

165 Art. 117 para 2 lit. f FC.

166 Art. 1 lit. c HGTA.

167 Art. 26 HGTA.

168 Art. 27 HGTA.

169 Art. 28 para 1 HGTA.

170 Swiss Federal Council, *Botschaft zum Bundesgesetz über genetische Untersuchungen beim Menschen vom 11. September 2002* (BBl 2002) 7361, 7438; Lanz (n 8) 23.

171 Art. 4 HGTA. Cf. Claudia Mund, *Grundrechtsschutz und genetische Information*, Basler Studien zur Rechtswissenschaft, vol 71 (Helbing Lichtenhahn 2005) 266ff.

4. Right to respect one's personality

52 There is no general prohibition of discrimination in Swiss private law.[172] Legal scholars, however, derive such a protection from the right to respect one's personality enshrined in Art. 28 of the Civil Code (CC).[173] It is argued, for example, that this provision could act as an indirect prohibition of discrimination under private law, because unequal treatment on the basis of characteristics of a person which are protected by the right to respect one's personality constitutes a violation of personality.[174] Other scholars even derive a right to non-discriminatory treatment from the right to respect one's personality.[175]

53 It is not immediately clear which characteristics are to be taken into account when determining discrimination as a violation of the right to respect one's personality, since the protection of this right is not limited to certain characteristics of a person but protects the personality as a whole. However, it seems logical to construe the relevant characteristics for a violation of personality with the protected characteristics mentioned in the non-discrimination principle in the Federal Constitution.[176] In fact, the constitutionally protected characteristics, such as gender, nationality, race, age, state of health, sexual preferences, political views or religious affiliation, are regularly referenced in the literature.[177] As always, a certain severity of the impairment is required as a threshold for a violation of personality.[178] To give an example, the Federal Supreme Court has stated that only an offensive disregard of an employee's personality will qualify as discrimination against that employee.[179]

54 It is generally accepted that a discriminatory contract formation can also be qualified as a violation of personality.[180] Discrimination is inadmissible not only if the conclusion of a contract is refused, but also if a contract is concluded on less favourable terms for reasons that are unrelated to the subject of the contract and that are infringing the right to respect one's personality.[181] This may be the case when insurance contracts are individualised, in particular when the conditions are determined on the basis of gender, age or nationality.

55 However, personality-infringing discrimination can be justified, namely by an overriding private interest.[182] This is the case if the insurance company can show objective reasons for individualisation based on protected characteristics which outweigh the interest in not being evaluated based on such characteristics.[183] If an offer is individualised on the basis of the risk profile, this should qualify as justifying overriding private interest. The same holds true when the premium is calculated with regard to the willingness to pay. In both constellations it is decisive that the individualisation is not based on a protected characteristic, but on other criteria. A mere correlation of risk profile or willingness to pay with a protected characteristic will therefore not establish an unlawful violation of personality.

172 Ruth Arnet, *Freiheit und Zwang beim Vertragsschluss* (Stämpfli Verlag 2008) para 356; Andreas Bucher, *Natürliche Personen und Persönlichkeitsschutz* (Helbing Lichtenhahn 2009) para 433; for an overview cf: Tarek Naguib, 'Diskriminierende Verweigerung des Vertragsabschlusses über Dienstleistungen Privater: Diskriminierungsschutz zwischen Normativität, Relativität und Idealität' (2009) Allgemeine Juristische Praxis, 993, 1005; Bettina Hürlimann-Kaup/Jörg Schmid, *Einleitungsartikel des ZGB und Personenrecht* (Schulthess 2016) para 1100; Samantha Besson, *L'égalité horizontale: l'égalite de traitement entre particuliers* (Fribourg: Editions Universitaires 1999) para 1240 ff.; Herbert Trachsler, *Das privatrechtliche Gleichbehandlungsgebot* (Dike 1991) 3ff. and 188ff.

173 Arnet (n 172) point 356; Peter Gauch and others, *OR AT: Band 1* (Schulthess 2014) para 1111; Tarkan Göksu, *Rassendiskriminierung beim Vertragsabschluss als Persönlichkeitsverletzung* (Freiburg: Universitätsverlag 2003) para 214ff.; Naguib (n 172) 1005ff.

174 Arnet (n 172) para 356.

175 Naguib (n 172) 1006; Pärli and others (n 48) 28.

176 See above, D.II.1.

177 Roger Zäch, 'Der Einfluss von Verfassungsrecht auf das Privatrecht bei der Rechtsanwendung' (1989) Schweizerische Juristen-Zeitung, 25, 26; Peter Gauch and others (n 173) para 1111. By referring to these criteria, specific, personality-forming and often unchangeable characteristics are qualified as relevant; some authors argue that the impairment of such characteristics is a pre-requisite for the existence of discrimination (Tarkan Göksu, 'Drittwirkung der Grundrechte im Bereich des Persönlichkeitsschutzes' (2009), Schweizerische Juristen-Zeitung, 89, 99).

178 Heinz Hausheer and Regina E. Aebi-Müller, *Das Personenrecht des Schweizerischen Zivilgesetzbuches* (Stämpfli Verlag 2016) point 12.06; Andreas Meili, 'Art. 28 ZGB' in: Heinrich Honsell and others (eds) *Basler Kommentar Zivilgesetzbuch I: Art. 1-456 ZGB* (Helbing Lichtenhahn 2014) para 38; Regina E. Aebi-Müller, 'Art. 28 ZGB' in: Peter Breitschmid and Alexandra Rumo-Jungo (eds), *Handkommentar zum Schweizer Privatrecht, Personen- und Familienrecht, Partnerschaftsgesetz: Art. 1-456 ZGB, PartG* (Schulthess 2016) para 3; Sibylle Hofer and Stephanie Hrubesch-Millauer, *Einleitungsartikel und Personenrecht* (Stämpfli Verlag 2012) point 20.11.

179 Swiss Federal Court (BGE 129 III 276) [2003] at 3.1.

180 Peter Gauch and others (n 173) para 1111; Göksu (n 173) point 274 ff., 312; Naguib (n 172) 1005ff; Arnet (n 172) point 357 and 363; Zäch (n 177) 25ff.; with regard to insurance law: Stephan Hartmann, 'Der Schutz der Versicherten vor Missbräuchen im revidierten Aufsichtsrecht' (2007) Haftung und Versicherung, 30, 33, with further references.

181 Göksu (n 173) para 199ff; Peter Gauch and others (n 173) para 1111a.

182 Art. 28 para 2 ZGB.

183 Arnet (n 172) para 371. For the balancing of interests in the context of justification see also: Hofer and Hrubesch-Millauer (n 178) para 2069; Hausheer and Aebi-Müller (n 178) para 12.23; Aebi-Müller (n 178) 32.

56 If, however, there is no justification, the person whose personality has been infringed is not only entitled to injunctive relief, damages and satisfaction,[184] but also to the conclusion of a contract on non-discriminatory terms.[185]

III. U.S./California

1. Federal Anti-discrimination Law

57 In the U.S., the constitutional prohibition of discrimination is only binding on governmental units and officers and does not apply to private insurers.[186] However, next to this constitutional prohibition, there is a variegated body of anti-discrimination laws consisting of federal laws and state regulations applying to businesses and legal entities.[187] Some of these laws are pertinent to the business of insurance as they limit the types of permitted discrimination. These are ACA, HIPAA and the Genetic Information Nondiscrimination Act (GINA).[188] These acts are the only federal laws expressly forbidding insurers from engaging in any form of discrimination in the underwriting process. On the federal level, there is no general prohibition for insurance companies to take, for example, race, religion, or national origin into account.[189] Moreover, employers offering health insurance to their employees have to comply with the Civil Rights Act[190] and the Americans with Disabilities Act (ADA),[191] which prohibit discrimination based on various protected characteristics.[192] Each of these Acts enumerates some prohibited grounds for discrimination (e.g. race, gender, health status), but there is no centralised agency for enforcing respective discriminatory cases.[193]

a.) U.S. Constitution

58 Under the U.S. constitution, a common characteristic of a group, such as skin colour, gender, or sexual orientation, ought not to form the basis for unequal treatment. This principle is enshrined in the Equal Protection Clause of the Fourteenth Amendment to the U.S. Constitution.[194] Equally there are various other guarantees against certain types of discrimination found in the several Amendments of the U.S. Constitution.[195]

59 With the exception of Part C, Medicare health care coverage is managed by the federal government.[196] All governmental units are bound by the constitutional prohibition of discrimination. This includes those involved in Medicaid administration on a state level, such as CMS, which is responsible for review and approval of the state plans.[197]

b.) Patient Protection and Affordable Care Act (ACA)

60 The Patient Protection and Affordable Care Act (ACA), among others, aims at guaranteeing non-discrimination in connection with programmes funded under the ACA.[198] Therefore, the ACA prohibits discrimination on the basis of race, colour, national origin, sex, age, or disability in certain health programmes and activities.[199] The ACA also prohibits discriminatory premium rates for health insurance in the individual or small group market. Rating is limited to age, geographic area, individual or family unit, and tobacco use.[200] Only these listed factors may be taken into account in setting health insurance premiums, while the maximum premium variations that an insurer can charge for these factors are also determined by the ACA.[201] For

184 Art. 28a para 1 no. 1 f. and para 3 ZGB.

185 Peter Gauch and others (n 173) para 1111; Arnet (n 172) para 417ff; Göksu (n 173) para 660.

186 Julie C. Suk and Fred L. Morrison, 'The United States', in: Marie Mercat-Bruns (eds) *Comparative Perspectives on the Enforcement and Effectiveness of Antidiscrimination Law* (Springer 2018) 513, 513.

187 Avraham and others (n 5) 216; Suk and Morrison (n 186) 513ff.

188 The Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff.

189 Avraham and others (n 5) 199.

190 Civil Rights Act of 1964, 42 U.S.C. § 1981.

191 Americans with Disabilities Act of 1990, 42 U.S.C. § 12101.

192 Cf. Croskey and others (n 67) para 706 and 710.

193 Suk and Morrison (n 186) 514.

194 U.S. Constitution Amendment XIV. Peter J. Rubin, 'Equal Rights, Special Rights, and the Nature of Antidiscrimination Law' (1998) Michigan L.Rev. 97:564, 568; Avraham and others (n 5) 216.

195 Barbara J. Van Arsdale and others, 'Civil Rights', *American Jurisprudence* (2nd edn, August 2018 Update) para 3.

196 U.S. Government, Department of Health & Human Services, *Medicare & You* (2019, Centers for Medicare & Medicaid Services) <www.medicare.gov/Publications/>. Cf. above, C.III.1.a), for a general explanation of Medicare and Medicaid.

197 Cf. Furrow and others (n 29) 490.

198 42 U.S.C. § 18116; Stoltzfuss Jost (n 104) para II[HH][6].

199 45 C.F.R. §§ 92.1-92.303; Robert E. Anderson and others, 'Insurance', *American Jurisprudence 2d* (February 2019 Update) para 544.

200 42 U.S.C. § 300gg.

201 Avraham and others (n 5) 198 Fn. 6; In terms of age, the rate shall not vary by more than 3 to 1 for adults (42 U.S.C. § 300gg(a)(1)(A)(iii)). The rating factor tobacco use shall not

example, the factor "gender" is not on this list and therefore cannot be considered by health insurers.[202] Moreover, the insurers also have to consider all insureds of the individual and small group market to be members of the same risk pool.[203]

61 With respect to group or individual health insurance coverage, the exclusion based on pre-existing conditions or the discrimination of those who have been sick in the past is also explicitly prohibited under the ACA.[204] Hence, private health insurers must accept all applicants without regard to pre-existing conditions.[205] Furthermore, group health plans must not discriminate against individuals based on health status, medical conditions, medical history, genetic information or the like[206] or discriminate in favour of higher salaries.[207]

62 When interpreting the ACA's underlying race and sex statutes, courts have held that they only bar direct but not indirect discrimination. Nevertheless, district courts have been unwilling to completely dismiss the viability of indirect disability discrimination.[208] Accordingly, it is not yet excluded that ACA's anti-discrimination provision might also protect individuals against indirect discrimination.

c.) Health Insurance Portability and Accountability Act (HIPAA)

63 The Health Insurance Portability and Accountability Act (HIPAA) limits insurance companies' discretion in considering pre-existing conditions in the underwriting process for group health insurance coverage.[209] However, only some provisions of HIPAA are still relevant, due to fact that the ACA largely supersedes HIPAA.[210] To give an example, HIPAA's prohibition of discrimination based on health status in eligibility for coverage or premiums in older group health plans is still of relevance.[211]

vary by more than 1.5 to 1 (42 U.S.C. § 300gg(a)(1)(A)(iv)), see above, C.III.1.c).

202 Avraham and others (n 5) 198 Fn. 6.

203 42 U.S.C. § 18032(c); see above, C.III.1.c).

204 42 U.S.C. § 300gg-3.

205 DiMugno and Glad (n 104) para 37A:3.

206 42 U.S.C. § 300gg-4.

207 42 U.S.C. § 300gg-16(a); see: Anderson and others (n 199) para 544.

208 Cf. *Briscoe v. Health Care Services Corporation,* 2017 WL 5989727 (N.D.Ill. Dec. 4 2017); *Express Scripts v. Anthem ERISA Litigation*, No. 16 Civ. 3399 (ER) 2018 WL 339946 (S.D.N.Y. Jan. 5, 2018), appeal filed.

209 29 U.S.C. § 1181; Avraham and others (n 5) 198ff. with further references.

210 Furrow and others (n 29) 351.

211 Furrow and others (n 29) 351.

d.) Genetic Information Nondiscrimination Act (GINA)

64 The Genetic Information Nondiscrimination Act (GINA) prohibits discrimination in health insurance coverage and employment based on genetic information.[212] Health insurance providers are prohibited from requiring or requesting genetic information of the person insured or the individual's family members and may not use such information for fixing rates, decisions on granting coverage or to infer on pre-existing conditions.[213] Therefore denying coverage or charging different premiums to insureds based on genetic information is prohibited in group health insurance.[214] But disparate impact claims, i.e. cases involving indirect discrimination, are not included in GINA.[215]

e.) Civil Rights Act

65 The 1964 Civil Rights Act's Title VII[216] prohibits employers from imposing discriminatory terms and conditions upon employees. If employers provide health care coverage for employees, discrimination based on various protected characteristics is prohibited.[217] These protected characteristics are race, colour, religion, sex (including gender and pregnancy) and national origin.[218] Title VII of the Civil Rights Acts bars both direct and indirect discrimination.[219]

f.) Americans with Disabilities Act (ADA)

66 People with disabilities are guaranteed the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation. Notably, insurance

212 29 U.S.C. § 1182(b)(3); Thomas Wm. Mayo, 'Bioethics', in: American Health Lawyers Association (ed) *Health Law Practice Guide* (December 2018 Update, Clark Boardman Callaghan) para 15:16.

213 Mayo (n 212) para 15:16.

214 Avraham and others (n 5) 199; see: 29 U.S. Code § 1182; 42 U.S.C. § 300gg-1.

215 42 U.S.C. § 2000ff-7; Jennifer K. Wagner, 'Disparate impacts and GINA: Congress's unfinished business' (2018) 5 JLB 527, 530.

216 42 U.S.C. § 2000e et seq.

217 Croskey and others (n 67) para 706.

218 42 U.S.C. § 2000e-2; Tracy Bateman Farrell and others, 'Job Discrimination' American Jurisprudence (2nd edn, February 2019 Update) para 2.

219 42 U.S.C. § 2000e-2; Sara Rosenbaum, 'Insurance Discrimination on the Basis of Health Status: An Overview of Discrimination Practices, Federal Law, and Federal Reform Options' (2009) 37 J.L.Med.& Ethic, 101, 108.

offices, offices of health care providers, hospitals and other service establishments are, among others, qualified as public accommodation.[220] However, it is not clear whether the provisions of the Americans with Disabilities Act (ADA) apply to insurance policies and the underwriting practices of insurance companies.[221] If interpreted narrowly, insurance companies merely have to provide physical access to their service infrastructure. Such an interpretation would not impact the business model of an insurance company. By contrast, a broader interpretation would have a significant effect, as the respective provisions would apply to the goods and services offered by a public accommodation, meaning that disparate treatment of disabilities in an insurance policy's provisions or an insurer's underwriting decisions could be subject to scrutiny under the ADA. However, the literature notes that case law and the Justice Department's position on this matter have been inconsistent.[222]

2. Californian Anti-discrimination Law

67 The federal laws are supplemented by Californian state laws, which can be administered by state agencies.[223] Californian anti-discrimination regulations pertaining to the insurance business are found in the Constitution of California, the California Civil Code (CIV) and the California Insurance Code (INS).

a.) California Constitution

68 California's constitutional anti-discrimination regulation overlaps but is not identical with the equal protection principle of the U.S. Constitution.[224] The U.S. Constitution permits but does not require the state to grant preferential treatment to suspect classes,[225] whereas the Constitution of California prohibits the state from treating any individual or group differently in a positive or negative sense on the basis of race, sex, colour, ethnicity, or national origin in the operation of public employment, public education, or public contracting.[226] The notion of "state" includes political subdivisions and any department, division or sub-division of the state Government.[227] Therefore, any governmental agency has to comply with the constitutional anti-discrimination principle. This regulation is particularly important for the state administration of Medi-Cal and the CDI. Private insurers in California are not bound by this principle.

b.) California Civil Code (CIV)

69 According to the California Civil Code (CIV) all persons within the jurisdiction of California are free and equal.[228] Matters of sex, race, colour, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, sexual orientation, citizenship, primary language, or immigration status shall not play any role with regard to entitlements to full and equal accommodations, advantages, facilities, privileges, or services in all business establishments of every kind whatsoever. This provision applies to property-casualty insurances in California.[229] Therefore the aforementioned characteristics must not be considered when calculating automobile or renters insurance premiums.

c.) California Insurance Code (INS)

70 In Californian insurance law, discrimination on grounds of specific protected classes is prohibited.[230] By law, Californian insurance companies are prohibited from denying insurance coverage based on sex, marital status, race, ancestry, colour, religion, national origin, disability, medical condition, physical or mental impairment, genetic characteristics or sexual orientation.[231] The California Insurance Code (INS) expressly bars health insurers from discriminating on the basis of these

220 42 U.S.C. § 12181(7)(F).

221 Justice H. Walter Croskey and others, 'Chapter 11: Extracontractual Liability', *California Practice Guide: Insurance Litigation* (The Rutter Group 2017) para 351.

222 Cf. DiMugno and Glad (n 104) para 5:5; Croskey and others (n 221) para 351ff.

223 Suk and Morrison (n 186) 514.

224 B.E. Witkin, 'Chapter X. Constitutional Law' in: *Summary of California Law* (11th edn, Witkin Legal Institute 2018) para 1088(5)(c), with further references.

225 Witkin (n 224) para 1088(5)(c) and para 1089(a); cf. Rachel M. Kane, 'Public Works and Contracts', *California Jurisprudence 3d* (February 2019 Update) para 14.

226 Cal. Const., art. I, § 31(a)); Kane (n 225) para 14.

227 Witkin (n 224) para 1088(1).

228 § 51(b) CIV.

229 INS §§ 679.70 and 679.71 as well as 1861.03(a); DiMugno and Glad (n 104) para 66:18.

230 Kristina Alexander and others 'Issuance of Insurance Policies', in: Hinshaw & Culbertson LLP and Kristina Alexander (eds) California Insurance Law & Practice (Matthew Bender 2018) para 9.08[2][b].

231 Cf. INS § 679.71 for renters insurance, INS §§ 11628-11629.5 for automobile liability insurance, INS § 10140 for health insurance, NS §§ 10192.11(a)(1), 10192.11(h)(1), 10192.12(a)(2) and 10192.24(a). for Medicare supplement insurance and 10 CCR § 2560.3 which applies to all classes of insurance. Kristina Alexander and others (n 230) para 9.08[2][b].

characteristics.[232] Considering sexual orientation as an underwriting criteria or using it to determine whether to require an HIV-test is also prohibited. Even if insurers were to infer sexual orientation from marital status, living arrangements, occupation, sex, beneficiary designation, ZIP Codes or other territorial classification, this would qualify as an unlawful discrimination.[233] However, charging differing health insurance premiums for different sexes is allowed if it is based on objective, valid, and up-to-date statistical and actuarial data or sound underwriting practices.[234] Furthermore, adjusting health insurance rates for the same coverage, solely because of a physical or mental impairment, is prohibited unless the differentiation is based on sound actuarial principles or is related to actual and reasonably anticipated experience.[235]

71 For property-casualty insurances, Proposition 103 prohibits unfairly discriminatory insurance rates.[236] But there are no rules that specify how the "unfairly discriminatory" nature of rates shall be determined, since this concept is neither defined in the INS, nor in other regulations.[237] Therefore the CDI must make a case-by-case assessment.[238] Rates are deemed unfairly discriminatory whenever price differentials fail to reflect the difference in expected losses and expenses in an equitable manner.[239]

IV. Findings

72 In Switzerland, the prohibitions of discrimination in the Federal Constitution and various statutes set certain limits to the individualisation of insurance contracts. Also, insurance companies are barred from utilising pre-symptomatic or pre-natal genetic tests in their underwriting procedures. Other forms of discrimination could be present if the individualisation is based on protected characteristics – such as age, gender or origin – and the differentiation cannot be justified on objective grounds. However, insurance companies individualise their conditions primarily according to the risk profile of the insured, and sometimes according to their willingness to pay. These factors do not usually align with protected characteristics. If they do so (as in the case of gender), insurance companies should be able to justify the individualisation on a regular basis as it will be based on objective reasons (e.g. higher risks of male drivers) and most often on actuarially sound criteria such as a different risk profile. Thus, there are hardly any relevant restrictions to the individualisation of insurance contracts arising from the general prohibition of discrimination.

73 In contrast to Swiss law, U.S. and Californian law provide strong and extensive protection against discrimination. These provisions are also applicable in horizontal relationships, i.e. they also govern contractual relationships between individuals and businesses. Californian insurance law prohibits discrimination and the use of certain protected characteristics for the insurer's risk classification. This regulation is in line with federal law, which prohibits discrimination in many sectoral laws for specific areas of insurance. Accordingly, the individualisation of insurance contracts must not be based on protected characteristics, further restricting the leeway for the individualisation of insurance contracts, which is already severely limited by insurance law. However, anti-discrimination law only rules out individualisation based on protected characteristics, thereby leaving (very limited) room for an individualisation based on other features.

E. Data Protection Law

I. Preliminary Remarks

74 For the individualisation of insurance contracts, insurers rely on data on their current or potential policyholders. The sources from which this data can be obtained are very diverse. Insurers have always demanded pre-contractual disclosure of information directly from the potential policyholder. But with the possibilities offered by new technologies, they can now increasingly rely on data collected during the term of the insurance contract (e.g. by using tracking tools) and on data bought from third parties, such as providers of social networking sites or apps.

75 The data analysed for the individualisation of insurance contracts will always be personal data and hence raise questions with regard to privacy and data protection law. The European approach to informational privacy has been and still is all-encompassing. European data protection laws apply to any processing of personal data in the public and the private sector,[240] thereby trying to establish

232 INS §§ 10140, 10143 and 10144.

233 INS § 10140(e).

234 INS § 10140(a).

235 INS § 10144.

236 See above, C.III.2.

237 De La Mora and Kook (n 116) para 6A.04(2), (4).

238 De La Mora and Kook (n 116) para 6A.04(2)-(4).

239 INS § 11732.5. In its assessments of rates, rating plans, and rating factors, the CDI applies a definition of "unfairly discriminatory" which was originally laid down in the law for workers compensation rates (De La Mora and Kook (n 116) para 6A.04(4).

240 Art. 2 para 1 GDPR; Art. 2 para 1 DPA.

rules and safeguards for all means and aims of processing personal data. The U.S. does not enact such all-encompassing data protection regulations, but rather pursues a sector-specific approach to safeguard informational privacy.[241]

76 In the past years, the data protection landscape has undergone significant changes, in particular due to the EU enacting the GDPR.[242] Switzerland is not an EU member state and under no formal obligation to implement the GDPR. However, Switzerland is a signee of the Council of Europe Convention 108 and when modernising the Convention 108 (Convention 108+) the Council of Europe ensured consistency with the GDPR.[243] Since Switzerland aims at signing the Convention 108+, it is set to adapt rules that align with the standard of the GDPR.[244] Furthermore, the GDPR claims to apply to processing activities outside of EU territory and hence businesses in Switzerland are often advised to ensure compliance with the GDPR. For these reasons, we will not limit the analysis of data protection law to the Swiss Data Protection Act (DPA),[245] but also include the GDPR.

77 The principles applied to the processing of personal data in Switzerland and the EU are only marginally different. However, there is one important (but often neglected) difference with regard to the regulatory approach: Under the GDPR every processing of personal data must have a lawful basis, such as consent of the data subject[246] or a legitimate interest of the controller;[247] in addition, the processing must be carried out in accordance with the applicable data protection principles.[248] In Switzerland, the processing of personal data is lawful if the data protection principles are respected and a lawful basis is only required if the handling of personal data is infringing these principles.[249]

II. Switzerland & the European Union

78 In Europe, data protection law is historically rooted in the right to respect for one's private and family life, his home and his correspondence.[250] The 1981 Council of Europe Convention for the protection of individuals with regard to the processing of personal data (Convention 108) established harmonised rules for electronic data processing. Nowadays, the right to data protection enjoys the status of a fundamental right in the EU[251] and, according to the predominant doctrine in Switzerland, the (fundamental) right to informational self-determination can be derived from the Swiss Federal Constitution.[252] The fundamental rights approach has led to European lawmakers enacting all-encompassing data protection laws, which apply to any handling of data relating to an identified or identifiable person.[253]

1. Data protection principles

79 European data protection laws set forth conditions for every processing of data that relates to an identified or identifiable person (personal data).[254] The notion of "processing" encompasses any handling of personal data one can think of.[255] Whoever, alone or jointly with others, determines the purposes and means of the processing of personal data is a "controller" and, among others, has to ensure being compliant with the principles relating to the processing of

241 Lothar Determann, 'Adequacy of data protection in the USA: myths and facts' (2016) 6 IDPL, 244, 246.

242 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

243 Council of Europe, *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Council of Europe, 2018) Treaty Series - No. 223, 1.

244 Swiss Federal Council, *Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017* (BBl 2017) 6941, 6969ff.

245 Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1.

246 Art. 6 para 1. lit. a GDPR.

247 Art. 6 para 1 lit. f GDPR.

248 Art. 5 GDPR.

249 Art. 12 para 2 lit. a DPA.

250 Art. 8 ECHR.

251 Art. 13 FC and Art. 8 Charter of Fundamental Rights of the European Union [2012] OJ C326/02.

252 Swiss Federal Court (BGE 138 II 346) [2012] at 8.2; Rainer J. Schweizer, 'Art. 13 BV' in: Bernhard Ehrenzeller and others (eds) *Die Schweizerische Bundesverfassung: St. Galler Kommentar* (Dike and Schulthess 2014) para 72; David Rosenthal, 'Art. 1 DSG' in: David Rosenthal and Yvonne Jhöri (eds) *Handkommentar zum Datenschutzgesetz* (Schulthess 2008) para 3ff. Critical: Eva Maria Belser, 'Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?', in: Astrid Epiney and others (eds) *Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung/Instruments de mise en oeuvre du droit à l'autodétermination informationnelle* (Schulthess 2013) 19.

253 Cf. Chris Jay Hoofnagle and others, 'The European Union general data protection regulation: what it is and what it means' (2019) 28 Info.&Comm.Tech.L., 65, 72ff.

254 Insurance companies have access to a variety of data sets and since the data can often be linked to individuals, it will qualify as personal data (cf. Weber (n 1) para 6).

255 Hoofnagle and others (n 253) 72ff.

personal data.[256] These principles are deemed the core of European data protection law.[257] As a general rule, every processing of personal data has to comply with all the data protection principles.[258]

80 Regarding the individualisation of insurance contracts based on big data analytics, the principles of purpose limitation,[259] data minimisation and storage limitation are of particular relevance.[260] Furthermore, questions with regard to the principles of fairness (translated as good faith in Switzerland) and transparency of processing arise.[261] Lastly, data quality can play a role in any data analysis.[262]

a.) Transparency and Purpose Limitation

81 The principle of transparency obliges controllers to be transparent with regard to their processing operations.[263] This principle is closely connected to the principle of purpose limitation as it requires the controller to provide information on the purpose of its processing.[264] The transparency of data processing is arguably not only the single most important principle of data protection law, but also the reason for the broad information duties of data controllers[265] and the right of access.[266]

82 The principle of purpose limitation is a key principle of data protection law and consists of two aspects: first, the purposes for which the controller intends to process the data need to be specified (purpose specification); and second, these purposes set the limits for the controller's processing operations (use limitation).[267] The purposes have to be clearly and unambiguously specified pursuant to the GDPR and a controller's processing operations are limited to what is compatible with these specified purposes. Swiss law allows processing for purposes that are specified or merely obvious due to the circumstances of the collection of the data. But in turn, a controller's operations are strictly limited to these purposes.[268]

83 In order to meet the requirements of transparency and purpose specification, insurance companies must ensure that their customers are aware of the fact that their personal data is processed for providing an individual offer, taking into account their personal risk profile and/or their willingness to pay. This should not cause particular problems with regard to data obtained directly from the (potential) policyholder in the context of a specific insurance contract. But insurance companies may want to use data that has not been obtained for the purpose of running big data analytics to calculate individual premiums, e.g. data on treatments and therapies collected for billing and reimbursement purposes. Such use would have to be classified as data repurposing[269] and would trigger the insurance companies' duty to inform the data subject accordingly. While informing their customers about such repurposing should not be a problem, it might be difficult or even impossible for insurance companies to comply with this requirement if their analysis includes data about individuals who are not their customers. As in other cases, the principle of transparency and purpose limitation appear to be in a fundamental conflict with big data analytics' idea of gaining new insights from existing data.[270]

256 Cf. Art. 5 para 2 GDPR; Switzerland currently employs a different terminology, yet it is expected that this will change.

257 Cf. Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/ 46/ EC and the General Data Protection Regulation' in: Marise Cremona (ed) *New Technologies and EU Law* (OUP 2017) 127 and 131.

258 Art. 5 GDPR; Art. 4 and 5 DPA. Peter Carey, 'Data Protection Principles' in: Peter Carey (ed) *Data Protection: A Practical Guide to UK and EU Law* (5th edn, OUP 2018) 32, 32.

259 Art. 5 para 1 GDPR; Art. 4 para 3 DPA.

260 Art. 5 para 1 lit. c and e GDPR; in Switzerland data minimisation and storage limitation are derived from the general principle of proportionality enshrined in Art. 4 para 2 DPA. Cf. Weber (Fn. 52) 101; Rolf H. Weber, 'Big Data: Rechtliche Perspektive' in: Rolf H. Weber and Florent Thouvenin (eds) *Big Data und Datenschutz – Gegenseitige Herausforderungen* (Schulthess 2014) 17; Philippe Meier, *Protection des données* (Stämpfli Verlag 2011) para 673; Yvonne Prieur, 'Datenschutz und «Big Data-Geschäfte» auf dem Prüfstand' (2015) Allgemeine Juristische Praxis, 1643, 1649; Bruno Baeriswyl, ‚Art. 4 DSG', in: Bruno Baeriswyl und Kurt Pärli (eds) *Stämpflis Handkommentar Datenschutzgesetz* (Stämpfli Verlag 2015) para 23; Florent Thouvenin, ‚Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze' in: Volker Boehme-Nessler and Manfred Rehbinder (eds) *Big Data: Ende des Datenschutzes? Gedächtnisschrift für Matin Usteri*, (Stämpfli Verlag 2017) 27, 34.

261 Art. 5 para 1 lit. a GDPR; Art. 4 para 2 and para 4 DPA.

262 Art. 5 para 1 lit. d GDPR; Art. 5 DPA.

263 Art. 5 para 1 lit. a GDPR; Art. 4 para 4 DPA.

264 Art. 13 para 1 lit. c and Art. 14 para 1 lit. c GDPR; Florent Thouvenin, 'Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data', in: Rolf H. Weber and Florent Thouvenin (eds) *Big Data und Datenschutz – Gegenseitige Herausforderungen* (Schulthess 2014) 61, 64.

265 Art. 13ff. GDPR; Art. 14 and Art. 18a DPA.

266 Art. 15 GDPR; Art. 8 DPA.

267 Art. 5 para 1 lit. b GDPR; Art. 4 para 3 DPA; Carey (n 258) 34; Bart Custers and Helena Uršič 'Big Data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection' (2016) 6 IDPL, 4, 8; Thouvenin (n 264) 67.

268 Thouvenin (n 264) 67ff.

269 Custers and Uršič (n 267) 8.

270 Thouvenin (n 264), *passim;* cf. Paul MacDonnell, 'The European Union's Proposed Equality and Data Protection Rules: An Existential Problem for Insurers?' (2015) 35 Ec.Aff., 225, 233, stating that insurance companies using data mining techniques do not know what they will find until it is too late.

b.) Data Minimisation and Storage Limitation

84 According to the data minimisation principle, as few data as necessary, for the purposes of the processing shall be processed.[271] Similarly, the principle of storage limitation's objective is to ensure that controllers do not keep data longer than necessary for the initial purpose of the processing.[272] Thus, as few data as needed for the purposes specified at the initial collection shall be processed and as soon as the initial purpose of the collection is fulfilled, the personal data has to be deleted. As seen already, it is arguably impossible to be specific about the purposes of big data analysis. Since the data would have to be deleted as soon as the initial purpose is fulfilled, data reuse would be generally impossible according to these principles. Thus, if interpreted strictly, the data minimisation and storage limitation principles go head to head with big data analytics and many other data processing practices, since the data would have to be deleted and be lost for future analysis.[273] These challenges also affect the processing of personal data by insurance companies. Namely, the principles of data minimisation and storage limitation may have a negative impact on the accuracy of the data analysis carried out to determine individual risk profiles and willingness to pay, but they do not hinder the individualisation of insurance contracts as such.

c.) Data Quality

85 An important aspect of any data analysis is data quality. Data protection laws in Switzerland and the EU incorporate a data accuracy principle, according to which personal data must be accurate and, where necessary, kept up to date.[274] The principle intends to prevent decisions made on the basis of poor data. However, the controller should only alter and update data when it is necessary to mitigate potential dangers to the fundamental rights of the data subjects.[275] Whenever this danger cannot be identified, there is no need to "correct" or update the data. While ensuring data quality might be as difficult for insurance companies as for other data controllers, this principle does not hinder the individualisation of insurance contracts.

d.) Fairness and Good Faith

86 The principle of fairness or good faith[276] has a catch-all function.[277] It is understood as a duty to safeguard the interests of the data subject in good faith and not to interfere unnecessarily with his protected interests. Clandestine data processing as well as data processing which the data subject did not need to expect, often conflict with the principle of good faith.[278] Even though the principle of good faith might be affected in many constellations, its importance should not be overestimated. Scholars rightly argue that it should only be used restrictively to correct disturbing results that would otherwise be in accordance with the law.[279] Thus, the principle also has little steering effect regarding the interpretation of legal norms.[280] In particular, good faith should not be equated with an obligation to equal treatment or a general prohibition of differential treatment. Rather these prohibitions need to be specified in statutes.[281] Hence the principle of good faith does not hinder individualisation of insurance contracts.

2. Lawful basis

87 In the EU, data processing must always be based on (at least) one of six reasons for the lawfulness of processing.[282] In Switzerland, such reasons are only needed if the principles relating to the processing of personal data are violated.[283]

271 Art. 5 para 1 lit. c GDPR; Art. 4 para 2 DPA, where the principle of data minimisation is derived from the more general principle of proportionality; see Thouvenin (n 63) 31.

272 Art. 5 para 1 lit. e GDPR; Art. 4 para 2 DPA, where the principle of storage limitation is derived from the more general principle of proportionality; see Thouvenin (n 63) 31; for an EU perspective see also Tjimen H.A. Wjisman, 'Privacy, Data Protection and E-Commerce', in: Arno R. Lodder and Andrew D. Murray (eds) *EU Regulation of E-Commerce: A Commentary* (Edward Elgar 2017) point 12.13.

273 MacDonnell (n 270) 233; Hoofnagle and others (n 253) 78.

274 Art. 5 para 1 lit. d GDPR; Art. 5 DPA.

275 Cf. Thomas Hoeren ‚Big Data und die Datenqualität – ein Blick auf die DSGVO'(2016) 6 ZD, 459, 461ff.

276 Art. 5 para 1 lit. a GDPR; Art. 4 para 2 DPA.

277 Lee A. Bygrave, *Data Privacy Law* (OUP 2014) 146; Tobias Herbst, 'Art. 5 DS-GVO' in: Jürgen Kühling and Benedikt Buchner (eds) *Datenschutz-Grundverordnung/BDSG* (2nd edn, C.H. Beck 2018) para 17; David Rosenthal, 'Art. 4 DSG' in: David Rosenthal and Yvonne Jhöri (eds) *Handkommentar zum Datenschutzgesetz* (Schulthess 2008) para 14.

278 Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework* (Springer 2018) 88; Baeriswyl (n 260) para 19.

279 Thouvenin (n 63) 34; Herbst (n 277) para 17; Philipp Reimer, 'Art. 5 DSGVO' in: Gernot Sydow (ed) *Europäische Datenschutzgrundverordnung* (2nd edn, Nomos, Manz and Dike 2018) para 14; Alexander Roßnagel, 'Art. 5 DSGVO' in: Simitis and others (eds) *Datenschutzrecht: DSGVO mit BDSG* (Nomos 2019) para 47.

280 Roßnagel (n 279) para 48.

281 Thouvenin (n 63) 35.

282 Art. 6 GDPR.

283 Thouvenin (n 63) 36.

a.) Consent

88 Most often, the data subject's consent serves as a legal basis.[284] Consent must be freely and unambiguously given after adequate information on specified purposes of the processing operation.[285] Notably, consent to processing may be withdrawn by data subjects at any time without having to specify any reasons.[286] While this makes it difficult for controllers to rely on consent, the processing on other lawful bases remains possible.

89 Swiss and EU law contain hardly any formal requirements regarding consent. Neither law requires it to be given in writing. However, since a controller has the burden of proof when relying on consent for processing, he or she is advised to obtain consent in writing or another documentable form.[287] Unambiguous consent means that insurance companies may not rely on opt-out mechanisms, but actually require their customers to opt-in to the processing of their personal data.[288]

90 Regarding substantive requirements, the requirement of freely given consent is the one that limits controllers the most. In this context so-called bundling, i.e. making the performance of a contract conditional upon consent to the processing of personal data that is not necessary for the performance of that contract, is discussed controversially.[289] Some scholars argue that take-it-or-leave it choices do not qualify as a freely given consent.[290] However, one may also take the view that whenever providing personal data is part of the data's subject's main obligation, such processing is necessary and not prohibited by data protection law.[291]

91 With regard to insurance contracts, providing information that enables assessing risks in underwriting procedures is part of the insured's main obligation. The same can be said for data collected during the term of the contract. While data on the insured's behaviour related to the risks which are covered by the insurance contract may not be strictly necessary for the performance of the contract, this data is so closely linked to the insurance contract that requesting consent to collecting such data can hardly be qualified as bundling. The same is true for data on the data subject's willingness to pay. While there is no direct connection to the performance of the contract, such data is used to provide an individualised offer for entering into a specific contract and is thus so closely related to the contract that requesting consent for the processing of such data cannot be qualified as bundling. There might be bundling and no freely given consent, however, if the insurance company requests consent for collecting of data which is neither related to the risks covered by the insurance contract, nor to the insured's ability or willingness to pay.

92 Since consent is only valid with regard to the specific purpose for which it was given, controllers need to get renewed consent if they want to process personal data for other purposes than the one it had been collected for.[292] As mentioned above,[293] this emanation of the principle of purpose limitation goes head to head with the idea of big data analytics to analyse data for other purposes than the ones initially intended. However, the limitation is not strict. While the GDPR allows the processing for compatible purposes, the DPA allows processing for purposes that were indicated by the controller or obvious from the circumstances.[294] While it remains unclear what purposes would qualify as "obvious" under Swiss law, the GDPR states which criteria must be taken into account to assess the compatibility of a new purpose.[295] As the repurposing of data does not always need consent, the controller may use the data for big data analytics as far as the new purpose is compatible with the one for which the data was collected for.

93 The purposes for which insurance companies use personal data will most often be closely connected – at least as long as the data is used in the realm of one specific insurance contract; e.g. the processing of personal data to decide on whether the insurance company has to pay for an insured event (e.g. a car

284 Art. 13 para 1 DPA; Art. 6 para 1 lit. a GDPR.

285 Cf. Art. 4 para 11 GDPR and Art. 6 para 1 lit. a GDPR ; Art. 4 para 4 DPA. Corrado Rampini, 'Art. 13 DSG' in: Urs Maurer-Lambrou and Gabor P. Blechta (eds) *Basler Kommentar Datenschutzgesetz, Öffentlichkeitsgesetz* (3rd edn, Helbing Lichtenhahn 2014) para 3ff.

286 Art. 7 para 3 GDPR. Rampini (n 285) para 14.

287 Tobias Fasnacht, *Die Einwilligung im Datenschutzrecht* (Freiburg: Universitätsverlag 2017), Rn. 250 f.; Benedikt Buchner and Jürgen Kühling, ‚Art. 7 DS-GVO' in: Jürgen Kühling and Benedikt Buchner (eds) *Datenschutz-Grundverordnung/BDSG* (2nd edn, C.H. Beck 2018), para 27. Notably, the GDPR states that if consent is obtained in the context of a written declaration, it must be clearly distinguished from other matters, using clear and plain language (Art. 7 para 2 GDPR).

288 Hoofnagle and others (n 253) 79.

289 Art. 7 para 4 GDPR. For Switzerland cf. Rampini (n 285) para 8.

290 Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 28. November 2017) at 9ff.

291 Cf. C-673/17, *Planet 49*, Opinion of Advocate Szpunar [2019] (ECLI:EU:C:2019:246) at 99. As different notions of freedom could be applied in practice, it is to be seen from enforcement what courts deem acceptable "freedom" (Hoofnagle and others (n 253) 80).

292 Custers and Uršič (n 267) 8.

293 See above, E.II.1.a).

294 Art. 5 para 1 (b) and Art. 6 para 4 GDPR; Art. 4 para 3 DPA.

295 Cf. Art. 6 para 4 GDPR.

accident) and the use of such data for estimating the insured's (future) risk (e.g. his or her driving behaviour) are closely connected and these purposes should therefore be considered compatible. In addition, the data would remain in the controller-data subject relationship, so that the latter has a reasonable expectation of an insurance company using data on an insured event to amend and alter the terms of this relationship. Such forms of re-use would therefore not trigger the need to get renewed consent. It would be different, however, if data collected in connection with one contract (e.g. automobile insurance) is used for assessing the risks covered by a different contract (e.g. health insurance). In these cases, the insurance company would need to get the data subject's specific consent.

b.) Performance of a contract

94 Processing is lawful if it is necessary for the performance of a contract that the data subject is a party to, or to take steps to enter into a contract that the data subject has requested.[296] "Necessity" means that the purpose of the processing could not be fulfilled with anonymous information.[297] If the data is merely useful, this lawful basis shall not apply.[298] Controversially, the European Data Protection Board (EDPB) stated that only objectively necessary processing operations may be based on this legal ground and the contract cannot "artificially expand" the categories of personal data or processing operations beyond the data subject's reasonable expectations.[299] However, other scholars highlight that data may be processed if the purpose of the contract cannot "reasonably" be fulfilled by other means. Thus, they argue against a restrictive understanding of necessity and state that reducing costs and fostering efficiency are reasonable and hence necessary aspects of performing a contract.[300]

95 Certainly, insurers need comprehensive, granular and accurate data in order to assess the data subject's risks accurately. Thus, on the one hand it could be argued that the processing of any data facilitating the risk analysis is objectively necessary for the performance of the contract. On the other hand, business transactions can be performed in situations of uncertainty and such uncertainty is the very reason customers are willing to conclude insurance contracts. An insurer, it could therefore be argued, initially bears the risk of imperfect information and performing data analysis in order to reduce that risk with regard to individual customers could be deemed "unreasonable", since the insurer can always rely on risk groups and does not necessarily have to individualise insurance contracts. As establishing the necessity of processing for a contractual obligation comes with considerable uncertainties, controllers are advised to rely on other grounds for the lawfulness of processing.[301]

c.) Legitimate interests

96 In Switzerland and the EU, data processing can be based on an interest analysis.[302] Despite explicit interest analysis being regarded as a tool that would allow a judge to do the specific case justice,[303] in practice it is the controller who has to perform this balancing exercise.[304] In this interest analysis, the legitimate interests pursued by the controller are at the heart of the reasoning. But the interests of a third party may be taken into account as well.[305] These interests have to be legitimate, meaning that they shall be in accordance with the law in the broadest sense.[306] The controller's or a third party's interests

296 Art. 6 para 1 lit. b GDPR; Art. 13 para 2 (a) DPA.

297 Cf. C-524/06, *Huber* [2008] (ECLI:EU:C:2008:724) at 62ff; Estelle Dehon and Peter Carey 'Fair, Lawful and Transparent Processing', in: Peter Carey (ed) *Data Protection: A Practical Guide to UK and EU Law* (5th edn, OUP 2018), 42, 50.

298 Horst Heberlein, 'Art. 6 DS-GVO' in: Eugen Ehmann and Martin Selmayr (eds) *DS-GVO: Kommentar*, (2nd edn, C.H.Beck and LexisNexis 2018), para 13; Benedikt Buchner and Thomas Petri, 'Art. 6 DS-GVO' in: Jürgen Kühling and Benedikt Buchner (eds) *Datenschutz-Grundverordnung/BDSG* (2nd edn, C.H. Beck 2018), para 15.

299 European Data Protection Board, '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, version for public consultation' (EDPB, 9 April 2019) at 8ff.

300 These scholars reference GDPR, recital 39. Cf. Kai-Uwe Plath, 'Art. 6 DSGVO' in: Kai-Uwe Plath (ed) *DSGVO/BDSG: Kommentar* (3rd edn, Verlag Dr. Otto Schmidt 2018) para 20ff; Dehon and Carey (n 297) 55. Cf. Sebastian Schulz, 'Art. 6 DS-GVO' in: Peter Gola (eds) *Datenschutz-Grundverordnung: DS-GVO, VO (EU) 2016/679: Kommentar* (2nd edn, C.H. Beck 2018) para 38.

301 Hoofnagle and others (n 253) 80.

302 Art. 13 para 1 DPA; Art. 6 para 1 lit. f GDPR. Cf. above, E.I for the systematic differences between the two approaches.

303 Swiss Federal Council, *Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988* (BBl 1988) vol II, 413, 460.

304 Cf. Andreas Sattler, 'From Personality to Property: Revisiting the Fundamentals of the Protection of Personal Data', in: Mor Bakhoum and others (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?* (Springer 2018) MPI Studies on Intellectual Property and Competition Law, vol. 28, 27, 36.

305 Irene Kamara and Paul de Hert, 'Balancing and the Controller's Legitimate Interest' in: Evan Selinger and others (eds) *The Cambridge Handbook of Consumer Privacy* (CUP 2018) 331; Dehon and Carey (n 297) 58; Constantin Herfurth, 'Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO' (2018) 8 ZD, 5144; David Rosenthal, 'Art. 13 DSG' in: David Rosenthal and Yvonne Jhöri (eds) *Handkommentar zum Datenschutzgesetz* (Schulthess 2008) para 7; Rampini (n 285) para 21.

306 Herfurth (n 305) 514; Paolo Balboni and others, 'Legitimate

have to be balanced against the interests of the data subject. In a first step, the necessity of the processing in question has to be ascertained. In the literature, necessity is usually defined negatively, meaning one has to ask whether it would be possible to pursue the legitimate interests in a less interfering manner with the data subject's right to data protection.[307] Once it has been established that the legitimate interest in question cannot be fulfilled by less-invasive means, the interests have to be balanced against in a second step.

97 Insurers have an interest in collecting and processing comprehensive, granular and accurate data on the insured's characteristics and behaviour related to the risks covered by the insurance contract and on their ability and willingness to pay. As this interest is backed by the controller's fundamental freedom to conduct business[308] and since it may be assumed that neither Switzerland nor the EU member states prohibit the processing of data for these purposes, the interest of the controller in having access to that data can be considered legitimate.

98 While many scholars and data protection authorities (implicitly) base the pondering of interests on the assumption that data subjects have a general interest in not having their data collected and processed, a person seeking out insurance may actually have an interest in the processing of his or her personal data for the purpose of individualisation as they may get a better offer if their risk profile and/or their willingness to pay is below average. Therefore, the balancing of interests must be nuanced: On the one hand, the portion of policyholders whose individual risks are smaller than the average risk of the group they would be part of actually benefits from the data processing. Their personalised premiums should be lower than the premiums they would have to pay when classified in a risk group. On the other hand, policyholders whose risks are higher than the average risk of their group have no interests in a personalised risk profile and insurance contract. Furthermore, persons who are not part of the data-controller-data-subject relationship would benefit from another individual's data being analysed as long as the analysed individual has a higher risk than they do. The more high-risk individuals pay individualised premiums, the more likely it is that the low risk individuals pay lower premiums and eventually benefit from the data processing. The same argument applies to the willingness to pay.

99 Following this train of thought leads to a situation where the interests of individuals that would pay more due to individualisation outweigh the controller's legitimate interests in analysing the data, whereas the processing of data relating to policyholders that are better off with individualised premiums could be justified with the legitimate interests of the controller and the concurring interests of these data subjects. Such an interpretation, however, cannot solve the issue at stake and must be rejected for two reasons: First, it merely focuses on an analysis of the potential advantages or disadvantages of the data processing and does not take into account the general interest of (some) data subjects in not having their data analysed, irrespective of the effect of such analysis. Second – and this is the crucial point – in order to determine whether a (potential) policyholder actually benefits from the analysis of his or her data, the policyholder's data would have to be analysed. Hence an a priori differentiation between "winners" and "losers" is impossible, and the lawfulness of the processing can thus only be determined after the data has already been processed. As a consequence, the lawfulness of processing of personal data for the individualisation of insurance contracts cannot be based on such a pondering of interests.

100 As mentioned above, public interests should be taken into consideration as well[309] – and in this case they could actually help to solve the dilemma. From this perspective, the individualisation of insurance contracts based on the processing of personal data is a meaningful way to help solve the problems of adverse selection and moral hazard.[310] Since the processing of personal data allows for the offering of individual premiums, insurance companies should now be able to also attract policyholders with a low risk profile, thereby gaining additional customers and making insurance coverage attractive to low risk individuals as well. This would help tackle the problem of adverse selection much better than the mere sorting of policyholders into different risk groups. The problem of moral hazard could be significantly mitigated if the collection and processing of personal data gathered after the conclusion of the insurance contract (e.g. by using driving or fitness trackers) is considered legitimate, since the risk of having to pay higher premiums due to risky behaviour would provide powerful incentives to policyholders to behave more carefully.[311] Finally, from a public policy perspective, it is hard to dispute the fact that the individualisation of insurance premiums has positive effects on the economy as a whole.[312]

interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection' (2013) 3 IDPL, 244, 254; Dehon and Carey (n 297) 57; Rampini (n 285) para 22.

307 Kamara and de Hert (n 305) 332.

308 Art. 16 EU Charter of Fundamental Rights; Art. 26 Swiss Federal Constitution.

309 Herfurth (n 305) 515.

310 See above, B.I.

311 See above, B.I.

312 See above, B.II.

101 In sum, there are good arguments for an overriding legitimate interest of the insurance companies which would ensure the lawfulness of processing of the insured's personal data. Nevertheless, since the balancing of interest analysis requires a case-specific assessment, it may be argued that a universal interest analysis is impossible. After all, an interest analysis should do justice to specific cases. As a consequence, insurance companies would run a considerable risk if they base the lawfulness of processing on their legitimate interests alone.

3. Special Categories of Data

102 In Switzerland, special categories of data enjoy additional protection as this data relates to the data subject's personality in a particularly sensitive way.[313] Such sensitivity is given if data relates to religious, ideological, political or trade union-related views or activities, health, the intimate sphere or the racial origin, social security measures, administrative or criminal proceedings, and sanctions.[314] However, the DPA does not prohibit the processing of such data per se. The aforementioned general conditions for lawfulness apply to special categories of data as well. While the controller may process such data in compliance with the data protection principles and he may rely on legitimate interests for justifying such processing if needed, there are some variations.[315] In particular, consent to processing special categories of data has to be express and, by statute, there is no legitimate interest in including special categories of data in creditworthiness checks.[316]

103 The GDPR prohibits the processing of special categories of data as defined in Article 9 of the GDPR, under the assumption that what is unknown cannot be used to discriminate.[317] Special categories of data are: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.[318] However, the law provides exemptions for neutral or desirable processing of these special categories of data, and allows the processing of such data with the data subject's explicit consent. While EU member states may enact further derogations,[319] neither legitimate interests nor necessity for the performance of a contract are a legitimate ground for the processing of special categories of data.[320]

104 These requirements and restrictions do not specifically relate to the individualisation of insurance contracts. But obviously they also have to be considered and met by insurance companies processing data that falls within one (or several) of these special categories.

III. U.S./California

1. Sector-Specific Data Protection Laws on a Federal Level

105 The situation with data privacy law in the U.S. is comparable to the situation regarding insurance law: the U.S. does not have a comprehensive data protection or data privacy law or any law regulating all issues of information privacy or security.[321] Also there is no direct expressed right of privacy in the U.S. Constitution or the Bill of Rights. But according to the U.S. Supreme Court, privacy is implicitly protected by the Constitution.[322] Moreover, the U.S. has many sector-specific federal laws regulating financial or health data or children's privacy.[323] Governmental agencies and industry groups also develop (self-regulatory) guidelines - so-called "best practices" - but in general these are not legally binding.[324] Notably, Section 5 of the Federal Trade Commission (FTC) Act declares unfair and deceptive acts or practices unlawful, with deception being the primary vehicle for privacy enforcement.[325] However, the FTC also enforces other privacy regulations.[326]

313 Gabor P. Blechta, 'Art. 3 DSG' in: Urs Maurer-Lambrou and Gabor P. Blechta (eds) *Basler Kommentar Datenschutzgesetz, Öffentlichkeitsgesetz* (3rd edn, Helbing Lichtenhahn 2014) para 27.

314 Art. 3 lit. c DPA.

315 Rosenthal (n 305) para 15.

316 Art. 4 para 5 DPA and Art. 13 para 2 lit. c DPA.

317 Benedikt Buchner, 'Art. 1 DS-GVO' in: Jürgen Kühling and Benedikt Buchner (eds) *Datenschutz-Grundverordnung/BDSG* (2nd edn, C.H. Beck 2018), para 14.

318 Art. 9 para 1 GDPR.

319 Art. 9 para 2 lit. g GDPR.

320 Cf. Art. 9 para 2 GDPR and Art. 22 para 2 GDPR.

321 Denis T. Rice, 'Challenges of Privacy Compliance and Litigation' in: Elizabeth M. Johnson and Jean Magistrale (eds) *Privacy Compliance and Litigation in California* (September 2017 update, Cal CEB) para 1.2.

322 *Griswold v. Connecticut*, 381 US 479 (1965); Clara Ruyan Martin and David B. Oshinsky, 'Privacy Law and Privacy Policy' in: Suzanne L. Weakley (ed) *Internet Law and Practice in California* (July 2017 update, Cal. CEB) para 9.7. See *Lawrence v. Texas*, 539 US 558 [2003]; *Roe v. Wade*, 410 US 113 [1973].

323 Kurt Wimmer, 'United States' in: Monika Kuschewsky (ed) *Data Protection & Privacy: International Series* (3rd edn, Thomson Reuters 2016), 1093, 1093.

324 Peter Swire and DeBrae Kennedy-Mayo, 'U.S. Private-Sector Privacy' (2nd edn, IAPP 2018) 58.

325 15 U.S.C. § 41.

326 See Swire and Kennedy-Mayo (n 324) 42ff.

106 In contrast to the EU, the U.S. does not have a default prohibition of data processing. Accordingly, the processing of personal data is allowed unless a sector-specific restriction or prohibition applies.[327] In addition to the sector-specific federal regulations, the individual states have laws of their own, many of them mapping respective federal laws. As a result, U.S. data privacy law is a complex patchwork of federal and state regulations, which covers different jurisdictions and different sectors.[328]

107 On the federal level, the Health Insurance Portability and Accountability Act (HIPAA),[329] the Gramm Leach Bliley Act (GLBA),[330] the Fair Credit Reporting Act (FCRA)[331] and the Genetic Information Nondiscrimination Act (GINA),[332] are relevant for insurers.[333]

a.) Health Insurance Portability and Accountability Act (HIPAA)

108 The Health Insurance Portability and Accountability Act (HIPAA), which was supplemented by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) in 2009,[334] provides for national standards to protect the privacy and security of healthcare information. The HIPAA regulations regarding information privacy are set forth in the HIPAA Privacy and Security Rule.[335] HIPAA regulates the use and disclosure of "protected health information" by covered entities.[336] Protected health information is defined as "individually identifiable health information".[337] The information has to be created or received by a health care provider, relate to health or the provision of health care, and there has to be reasonable grounds to believe that a person can be identified through the data.[338] HIPAA's Privacy Rule does not apply to de-identified data, meaning such information may be shared freely. Nevertheless HIPAA provides protection to a lesser degree with respect to data that is largely de-identified but may contain data which could enable re-identification (limited data set).[339] By regulation, limited data sets can only be shared for research, public health, and health care operations, but no other purposes.[340] Covered entities are health plans, health care clearinghouses and some health care providers.[341] The notion of "health plan" refers to an individual or group plan that provides or pays the cost of medical care. Health plan includes group health insurance and health insurance issuers, which are defined as a licensed and state-level regulated insurance company, as well as insurance service providers, and insurance organisations.[342] Most insurance companies are covered by this notion[343] and accordingly, health insurance policies are subject to HIPAA.

109 Covered entities have to comply with certain administrative, physical, technical and organisational security standards. For example they must ensure the confidentiality, integrity, and availability of electronic protected health information.[344] A covered entity may not use or disclose protected health information, unless permitted or required by the privacy rule or with written authorisation by the individual who is the subject of the information.[345] Protected health information may be used with the consent of the individual or for treatment, for payment, and for health care operations.[346] Generally, underwriting, enrolment, premium rating, and other activities in connection with health insurance contract formation or renewal, as well as with health

327 Lothar Determann, *California Privacy Law* (3rd edn, IAPP 2018) 38.

328 Wimmer (n 323), 1093; Rice (n 321) para 1.2.

329 Health Insurance Portability and Accountability Act of 1996, 26 U.S.C., § 9801.

330 The Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, 15 U.S.C. § 6801.

331 The Fair Credit Reporting Act, 15 U.S.C. § 1681.

332 The Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff., 42 U.S.C. § 2000ff.

333 The Federal Trade Commission Act (FTCA, 15 U.S.C. §§ 41-58.) would prohibit unfair or deceptive practices and is applied to consumer's offline and online privacy and data security policies. But, due to the McCarran Ferguson Act, the business of insurance is only within the FTCA's jurisdiction as far as it is not regulated by state law (15 U.S.C. § 1012).

334 Wimmer (n 323) 1100.

335 45 C.F.R. Part 160 and 164. Cf. Swire and Kennedy-Mayo (n 324) 167ff; Wimmer (n 323), 1100.

336 45 C.F.R. § 164.502(a). John T. Soma and others, *Privacy Law in a nutshell* (2nd edn, West Academic Publishing 2014) 114.

337 45 C.F.R. § 160.103.

338 Wimmer (n 323) 1094.

339 Determann (n 327) 148ff; see: 45 C.F.R. § 164.514(b) for the requirements for de-identification of protected health information and 45 C.F.R. § 164.514(e) for the requirements regarding limited data sets.

340 45 C.F.R. § 164.514(E)(3).

341 45 C.F.R. § 160.102(a).

342 Cf. 45 C.F.R. § 160.103. The notion of "health plan" also includes federal and state government health benefit plans, such as Medicare and Medicaid (Medi-Cal), but excludes workers' compensation insurers (Paul T. Smith, 'Health Information Privacy', in: Elizabeth M. Johnson and Jean Magistrale (eds) *Privacy Compliance and Litigation in California* (September 2017 update, Cal CEB) para 7.25).

343 Daniel J. Solove and Paul M. Schwartz, *Privacy Law Fundamentals* (2017 edn, IAPP 2017) 99.

344 45 C.F.R. § 164.306 (general security standards); 45 C.F.R. § 164.308 (administrative safeguards), 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 45 C.F.R. § 164.314 (organizational safequards); Determann (n 327) 150.

345 45 C.F.R. § 164.502(a).

346 45 C.F.R § 164.502.

benefits, qualify as such health care operations.[347] While use, disclosure and requests of protected health information shall be limited to the minimum necessary to accomplish the intended purposes of said operation, the use and disclosure of genetic information for underwriting purposes is entirely prohibited.[348] Finally, under HIPAA an individual has a right to be adequately notified (notice of privacy practice) of the possible uses and disclosures of its protected health information, as well as of its rights and the covered entity's legal duties with respect to protected health information.[349] In this notice of privacy practice, a health plan that uses protected health information for underwriting must include a statement that it is prohibited from using or disclosing genetic information for this purpose.[350]

b.) Gramm-Leach-Bliley Act (GLBA)

110 The Gramm-Leach-Bliley Act (GLBA) limits the disclosure of non-public personal information collected by a financial institution,[351] i.e. an institution engaging in activities which are financial in nature.[352] By statute, insuring against loss, harm, damage, illness, disability, or death is qualified as financial activity.[353] Therefore, insurance companies are subject to the GLBA. With regard to its material scope of application, the GLBA protects personally identifiable financial information that is provided by, results from, or is otherwise obtained in connection with consumers and customers who obtain financial products.[354] However, the Act is neither applicable to information in the public domain, nor to non-public financial information. With regard to substantive provisions, the GLBA imposes privacy and data security obligations on financial institutions. The Financial Privacy Rule foresees that privacy notices need to be provided to customers who obtain a financial product or service. Furthermore, certain restrictions on a financial institution's information sharing practices, as well as a duty to safeguard customer information (Safeguard Rule), are imposed.[355] The customer must be informed about the institution's privacy policies and practices *ab initio* and kept up-to-date at least annually.[356] In particular, information on the disclosure and protection of non-public information must be given.[357] The customers must also be informed about the possibility that their non-public personal information may be disclosed to a non-affiliated[358] third party and they must be given the opportunity to opt-out of having their non-public personal information shared with non-affiliated third parties, except for fraud prevention or the processing of consumer transactions.[359] Additionally, the financial institutions have to ensure the security of the customer's information and records. The latter must be protected against anticipated security threats or hazards and unauthorised access or use.[360]

111 Besides the relatively detailed rules on privacy policies and information sharing, the GLBA does not restrict the use of personal information and hence does not limit the possibilities of personalising insurance contracts based on big data.

c.) Fair Credit Reporting Act (FCRA)

112 The Fair Credit Reporting Act (FCRA)[361] shall protect consumers from inaccurate or unfair uses of their personal information in credit reports.[362] The Act regulates the disclosure and use of personal information supplied by Consumer Reporting Agencies (CRA),[363] and in particular the use of consumer reports[364] for adverse action.[365] Insurance companies might have an interest in consumer reports when individualising insurance contracts with regard to the willingness to pay. By statute, denial, cancellation, or other adverse

347 45 C.F.R. § 164.501.

348 45 C.F.R § 164.502(a)(5) and 45 C.F.R. § 164.502(b)(1).

349 45 C.F.R. § 164.520(a)(1).

350 45 CFR §§ 164.502(a) in connection with 164.520(b).

351 John T. Soma and others (n 336) 94.

352 15 U.S.C. § 6809(3)(A) and 12 U.S.C. § 1843(k).

353 Cf. 15 U.S.C. § 6809(3); 12 U.S.C. § 1843(k)(4)(B). 'Financial Data Privacy' in: Elizabeth M. Johnson and Jean Magistrale (eds) *Privacy Compliance and Litigation in California* (September 2017 update, Cal CEB) para 6.4.

354 15 U.S.C. § 6809(4), 16 C.F.R. § 313.3(o); Wimmer (n 323) 1094.

355 Wimmer (n 323) 1101.

356 15 U.S.C. § 6803.

357 15 U.S.C. 6803(a)(1)&(2) and 15 U.S.C. 6803(a)(3).

358 "*The term "affiliate" means any company that controls, is controlled by, or is under common control with another company.*" (15 U.S.C. § 6809(6)).

359 15 U.S.C. § 6802; Determann (n 327) 94.

360 15 U.S.C. § 6801(b). Johnson and Magistrale (n 353) para 6.13.

361 Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x.

362 15 U.S.C. § 1681.

363 Johnson and Magistrale (n 353) para 6.15; Pauline T. Kim and Erika Hanson, 'People Analytics and the Regulation of Information under the Fair Credit Reporting Act' (2016) 61 St. Louis U.L.J. 17, 21.

364 A consumer report is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living", which is used for determining the eligibility for credit, insurance, employment or other authorized purposes (15 U.S.C. § 1681a(d)).

365 Swire and Kennedy-Mayo (n 324) 188ff; Johnson and Magistrale (n 353) para 6.38.

or unfavourable change of coverage, as well as unfavourable changes of the charged amount of any insurance, are considered such adverse actions.[366] Thus the use of consumer reports by insurers would have to comply with the FCRA.[367]

113 A CRA may only furnish a consumer report in accordance with the instructions of the consumer, or when it has reason to believe that the requesting person has a permissible purpose to obtain a consumer report.[368] By statute, the underwriting of insurance is such a permissible purpose.[369]

114 Where an adverse action is taken based on information contained in a consumer report, the user of the report shall inform the consumer about this fact.[370] Whenever consumer reports are used for big data analytics and such analysis leads to an insurer taking an adverse action, the insurer has to inform the consumer. However, the FCRA does not apply to companies when they use data derived from their customer-relationship in their decision-making processes.[371] As long as all the data in the insurer's database is derived directly from the consumer and not from a consumer reporting agency, the FCRA would not prevent performing big data analytics.

d.) Genetic Information Nondiscrimination Act (GINA)

115 The Genetic Information Nondiscrimination Act (GINA) prohibits employers and health insurance companies from discriminating against individuals on the basis of genetic information.[372] Therefore companies should refrain from collecting genetic information unless it is absolutely necessary and permitted by law.[373] Health insurers, in particular, are not allowed to request or purchase genetic information for underwriting purposes or prior to an individual's enrolment under a plan or coverage in connection with this enrolment.[374] They may also not request an individual's family member to undergo genetic testing.[375] Furthermore, premiums may not be adjusted on the basis of genetic information.[376]

2. Californian Data Protection Law

116 As on the federal level, the state of California does (not yet)[377] have a comprehensive data protection or (informational) privacy law. So far, California has only enacted harms-based privacy legislation, meaning that merely statutory protection against specific threats as well as rules relevant to certain industries and groups of data subjects exist.[378]

a.) Californian Constitution

117 The Californian constitution grants all people certain inalienable rights, one of them being a right to privacy.[379] This right applies to the local government, to private entities and to individuals.[380] But neither the wording, nor its interpretation by courts, impose concrete compliance obligations on companies.[381] A cause of action based on a violation of the right to privacy is possible if three elements are present: a legally protected privacy interest; a reasonable expectation of privacy; and a serious invasion of the privacy interest.[382] Thus, companies should keep the constitutional right to privacy in mind, even if intrusive invasions of personal privacy are in line with specific statutes and common law principles.[383]

b.) Insurance Information and Privacy Protection Act (IIPPA)

118 The personal information of insurance applicants or policyholders is strictly regulated in California, in particular by the Insurance Information and Privacy

366 15 U.S.C. § 1681a(k)(1)(B)(i).

367 Cf. Determann (n 327) 101.

368 15 U.S.C. § 1681b; see: Determann (n 327) 103.

369 15 U.S.C. § 1681b(a)(3)(C).

370 15 U.S.C. § 1681m(a)(1)).

371 15 U.S.C. § 1681a(d)(2)(A)(i).

372 See above, D.III.1.d). GINA expressly made genetic information protected health information under HIPAA, thus GINA violations are treated and enforced as an unauthorised use or disclosure under HIPAA (cf. John T. Soma and others (n 336) 133.)

373 Determann (n 327) 145.

374 29 U.S.C. § 1182(c)(4)(C); 29 U.S.C. § 1182(d); Determann (n 327) 146.

375 29 U.S.C. § 1182(c).

376 29 U.S.C. § 1182(b)(3)(A).

377 See below, E.III.2.f).

378 Determann (n 327) 37. An overview of some of California's major privacy laws can be found here: State of California Department of Justice, 'Privacy laws' <https://oag.ca.gov/privacy/privacy-laws> accessed 12 June 2019.

379 1972 Cal. Const. Art. I, § 1.

380 Determann (n 327) 44; Roy G. Weatherup, 'Common Law and Constitutional Privacy Protection' in: Elizabeth M. Johnson and Jean Magistrale (eds) *Privacy Compliance and Litigation in California* (September 2017 update, Cal CEB) para 2.6; *Hill v. National Collegiate Athletic Assn.* 7 Cal.4th 1 (1994), 18-20.

381 Determann (n 327) 45.

382 *Hill v. National Collegiate Athletic Assn.* 7 Cal.4th 1 (1994), 35-3. Witkin (n 224) para 643(c); Determann (n 327) 46.

383 Determann (n 327) 45.

Protection Act (IIPPA).[384] The IIPPA's purpose is to establish standards for the collection, use, and disclosure of information gathered in connection with the insurance business, and to maintain a balance between the insurers' need for information and the public's need for fairness in insurance information practices.[385] The regulations apply to health and property-casualty insurance[386]

119 Among others, the act contains provisions regarding the notice of information practices to all applicants and policyholders in connection with insurance transactions,[387] the disclosure of personal or privileged information,[388] the right to access recorded personal information,[389] and the right to have recorded information corrected or a portion of it deleted.[390] Notably, the IIPPA restricts on what basis an adverse decision may rest.[391] By statute, declination and termination of insurance coverage as well as charging higher rates for property or casual insurance or offering higher than standard rates in health insurance qualify as adverse actions.[392] Information on preceding adverse underwriting decisions, the information that an individual previously obtained insurance coverage through a residual market mechanism, and information possibly stemming from insurance-support organisations shall not be used as a basis for an adverse action.[393] Thus the information an insurance company can base an adverse underwriting decision on is limited. Furthermore, IIPPA also vests the insured with a right to receive reasons for an adverse underwriting decision.[394]

c.) California Confidentiality of Medical Information Act (CMIA)

120 The California Confidentiality of Medical Information Act (CMIA)[395] protects the privacy of California residents' medical information.[396] Any individually identifiable information regarding a patient's medical history, mental or physical condition, or treatment in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor, is protected.[397] The CMIA applies to providers of health care and their contractors and to health service plans.[398] Health insurers must comply with the Act.[399] In 2014 the CMIA was amended to cover providers of software and hardware that allow customers to manage their health,[400] making it applicable to wearables.

121 The use or disclosure of health information "for any purpose not necessary to provide health care services to the patient," is prohibited unless the individual has given his consent, or it is otherwise permitted by the CMIA. For example, the disclosure to an insurer for the payment of services is permitted by statute.[401] If an insurance company receives medical information from a person or company that is subject to the CMIA, it may not further disclose this information except in accordance with a new authorisation that meets the requirements of the CMIA.[402] However, the CMIA does not prevent the disclosure of medical information by a provider of health care to an insurance institution subject to the IIPPA, provided the institution has complied with all requirements for obtaining the information set forth by IIPPA.[403]

d.) California Financial Information Privacy Act (CFIPA)

122 The California Financial Information Privacy Act[404] (CFIPA) makes use of the GLBA's reservation for states wishing to expand and tighten its rules on financial privacy protection.[405] The CFIPA requires financial institutions[406] to obtain written consent from a customer before disclosing said customer's non-public personal financial information.[407] In some cases, CFIPA mandates that this consent must be provided by an affirmative action (opt-in),

384 INS §§ 791-791.29.

385 INS § 791.

386 INS § 791.01.

387 INS § 791.04.

388 INS §§ 791.06, 791.13.

389 INS § 791.08.

390 INS § 791.09.

391 INS § 791.12; Witkin (n 32) para 541.

392 INS § 791.02(a)(1)(A), (B), (D) and (E).

393 INS § 791.12.

394 INS § 791.10.

395 CIV §§ 56-56.37.

396 Cf. Determann (n 327) 156.

397 CIV § 56.05(j).

398 Determann (n 327) 156; see: CIV §§ 56.05(m) in connection with 56.06. Cf. Fn. 69.

399 Determann (n 327) 157.

400 CIV §§ 56.06; Determann (n 327) 157.

401 CIV §§ 56.10; cf. Paul T. Smith (n 342) para 7.4.

402 CIV § 56.13; cf. Determann (n 327) 158.

403 CIV § 56.10(c)(11).

404 California Financial Code (FIN) §§ 4050 – 4060.

405 FIN §§ 4051.5(a); Swire and Kennedy-Mayo (n 324) 204; Johnson and Magistrale (n 353) para 6.47.

406 Financial institution is defined as it is in the GLBA, 15 U.S.C. § 6809(3)(A) as well as FIN § 4052(c) refer to 12 U.S.C. § 1843(k).

407 Non-public personal financial information is defined the same way as under the GLBA, compare: 15 U.S.C. § 6809(4) and FIN § 4052(a).

whereas, in general, opt-out consent would be sufficient pursuant to the GLBA.[408] The written consent (opt-in) of the consumers must be obtained, if financial information shall be disclosed to third parties that are neither affiliates nor financial institutions for the purpose of offering non-financial products and services.[409] However, when disclosing non-public personal information to an affiliate, a health insurer must only provide the insured with an opt-out option and remind them annually in writing that the information is being disclosed.[410] An opt-out notice must also be sent if a financial institution wants to share financial information with another (non-affiliated) financial institution for the purpose of offering financial products or services.[411] However, under the CFIPA financial institutions are not required to obtain a consumer's consent for sharing non-medical, non-public information with their fully owned subsidiaries, as long as they are engaged in the same line of business and regulated by the same functional regulator.[412]

123 Insurers would be interested in non-public financial information for individualising insurance contracts in accordance with the willingness to pay. In such a scenario the CFIPA's requirements regarding the disclosure of non-public personal information need to be observed. Opt-out and opt-in requirements do limit the information on which the individualisation of insurance contracts may be based with regard to individuals that object to their information being shared. But as far as the individualisation is based on non-public financial information already in possession of an insurer or its subsidiaries, the CFIPA does not limit the leeway for individualisation.

e.) Consumer Credit Reporting Agencies Act (CCRAA) and Investigative Consumer Reporting Agencies Act (ICRAA)

124 The Consumer Credit Reporting Agencies Act (CCRAA)[413] and the Investigative Consumer Reporting Agencies Act (ICRAA)[414] govern how consumer credit reporting agencies furnish information and reports for the needs of commerce. They require that such agencies need to adopt reasonable procedures and contain provisions concerning the confidentiality, accuracy, relevancy, and proper utilisation of such information.[415] While the CCRAA regulates consumer credit reports[416] and thus concerns a person's creditworthiness,[417] the FCRA also applies to reports regarding a consumer's character, i.e., general reputation, personal characteristics, or mode of living.[418] To a large extent both Acts, the CCRAA and the ICRAA, duplicate federal law, while in addition many provisions may be pre-empted by the FCRA.[419] Thus the relationship between CCRAA and FCRA is very complex.

125 A consumer credit report under the CCRAA is any written, oral, or other communication of any information by a consumer credit reporting agency bearing on a consumer's credit worthiness, credit standing, or credit capacity, which is among others, used for insurance underwriting.[420] Overall the CCRAA defines terms similarly to the FCRA and contains similar obligations for reports regarding someone's creditworthiness.[421] As is the case under the FCRA, whenever a CRA has reason to believe that a person intends to use a consumer report in connection with the underwriting of insurance, it may furnish said report to that person.[422] If information in a consumer credit report leads to adverse action with respect to any consumer, he or she also has to be provided with an adverse action notice.[423]

126 Investigative consumer reports as regulated in the ICRAA are reports in which information is obtained on a consumer's character, general reputation, personal characteristics, or mode of living.[424] This definition is broader than the definition of investigative consumer reports contained in the FCRA, since it includes information obtained "through any means"[425], while under the FCRA, the information is obtained through personal interviews only.[426]

127 The ICRAA's rules are stricter than the CCRAA rules pertaining to consumer credit reports.[427] An investigative consumer report may only be

408 Johnson and Magistrale (n 353) para 6.47.

409 FIN § 4053; Determann (n 327) 97.

410 FIN § 4053(b); Johnson and Magistrale (n 353) para 6.48.

411 Determann (n 327) 99. This financial product must be offered by at least one of the institutions, the receiving institution must be clearly identified and maintain the information confidentiality (cf. Johnson and Magistrale (n 346) para 6.48).

412 FIN § 4053(c); Determann (n 327) 98ff.

413 CIV §§ 1785.1-1785.36.

414 CIV §§ 1786 - 1786.60.

415 CIV § 1785.1(d) and CIV § 1786 (f).

416 CIV § 1785.3(c).

417 Johnson and Magistrale (n 353) para 6.50.

418 CIV § 1786.2(c).

419 Johnson and Magistrale (n 353) para 6.50.

420 CIV § 1785.3(c) in connection with CIV § 1785.11(a)(3)(C).

421 15 U.S.C. § 1681 a(e); Johnson and Magistrale (n 353) para 6.52.

422 CIV § 1785.11(a)(3)(C).

423 CIV § 1785.20.

424 CIV § 1786.2(c).

425 CIV § 1786.2(c).

426 Johnson and Magistrale (n 353) para 6.54.

427 Johnson and Magistrale (n 353) para 6.54.

prepared when a need for a specific purpose can be demonstrated, e.g. for determining eligibility or rates for insurance.[428] In general, the consumer needs to be informed a priori when an investigative consumer report is requested by the user.[429] Also a consumer has to give his consent if an investigative report that contains medical information shall be sent to an insurer.[430] If an insurance for personal, family, or household purposes increases the charge for insurance, or denies the consumer insurance based on a consumer's investigative consumer report, the insurance must inform the consumer and supply the name and address of the investigative consumer reporting agency that made the report.[431]

f.) Outlook: California Consumer Privacy Act (CCPA)

128 In 2018 a Californian ballot initiative for a comprehensive consumer privacy act enforced through litigation had received sufficient signatures to cast a vote. Since laws enacted through ballot initiatives are almost impossible to revise, the legislature was under pressure to present an indirect counter-proposal, which would make the initiators withdraw the ballot initiative. It was not until the last day of possible withdrawal that the Californian legislative hastily enacted the California Consumer Privacy Act (CCPA).[432] The CCPA will enter into force 1 January 2020 and will be supplemented by regulations issued by the Californian Attorney General on or before 1 July 2020.[433] This guidance will likely determine the scope of how the law is to be enforced in practice, since it is expected to elaborate on key definitions such as "personal information" and "unique identifiers", as well as procedures companies must have in place to effectuate the CCPA's consumer rights.

129 The CCPA protects "consumers", which are defined as California residents and the act thus applies to personal information relating to any California resident.[434] Companies that do business in California and either: (i) have an annual gross revenue of more than $25 million; (ii) receive or share personal information of more than 50,000 consumers, households, or devices; or (iii) derive more than 50 percent of their annual revenues from selling consumers' personal information have to comply with de CCPA.[435]

130 The CCPA regulates the selling of personal information and provides consumers with various rights. Selling is defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration".[436] However, businesses can claim that they are covered by one of several complexly specified exemptions from the definition of "selling".[437]

131 Consumers will have a right to be informed, to receive a privacy notice, and they will have access rights.[438] The information to be provided includes *inter alia* the categories of personal information collected about the consumer, the categories of sources and the categories of recipients.[439] Unlike the ballot initiative, consumers do not have a right to receive the name and identity of the data recipients.[440] Furthermore, consumers are vested with opt-out options, whereas minors have to opt-in to the collection of personal information.[441] The CCPA prescribes certain means of communication; for example, it requires businesses to communicate the opt-out option with consumers via a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information".[442] Furthermore, consumers have a right to get their data deleted.[443] Also companies must not discriminate against California residents on the basis of them exercising their rights under the CCPA by denying goods or services, charging different prices, or providing a different service quality. However, differing prices, rates or quality may still be applied, if these differences are

428 CIV § 1786.16(d) in connection with CIV § 1786.12(d)(2).

429 Johnson and Magistrale (n 353) para 6.54; CIV § 1786.16.

430 CIV § 1786.12(f).

431 CIV § 1786.40; Johnson and Magistrale (n 353) para 6.54.

432 CIV §§ 1798.100 -1798.199. Cf. Ian C. Ballon, 'Chapter 26 Data Privacy: 13A: Litigation Risks and Compliance Obligations under the California Consumer Privacy Act', in: Ian C. Ballon (ed) *E-Commerce and Internet Law: Legal Treatise with Forms* (2nd edn, 2019 Update, Thomson Reuters/West Publishing) vol 3, 26-401, Fn. 3; cf. Nicholas Confessore, 'The Unlikely Activist Who Took Silicon Valley – and Won' *NY Times Magazine*, (New York 14 August 2018) <www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>.

433 CIV 1798.185(a); Ballon (n 432) 26-402.

434 Lothar Determann, 'New California Law Against Data Sharing' (2018) 19 CRi, 117, 118; CIV § 1798.140(g).

435 CIV 1798.140(c). Christin McMeley and others, 'California Consumer Privacy Act: A Rapid Q&A' (2018) 23(7) Cyberspace Lawyer NL, 3.

436 CIV §§ 1798.140(t)(1).

437 Cf. Determann (n 434) 119; CIV §§ 1798.140(t)(2)A-D.

438 CIV §§ 1798.100, 1798.110, 1798.115.

439 CIV § 1798.110(a)(1), (2) and (3).

440 Thomas Hoeren and Stefan Pinelli, 'Das neue kalifornische Datenschutzrecht am Maßstab der DS-GVO: Auswirkungen des CCPA auf global agierende europäische Unternehmen' (2018) MMR, 711, 712.

441 CIV § 1798.120. Ballon (n 432) 26-406.

442 CIV 1798.135(a)(1).

443 CIV § 1798.105. Ballon (n 432) 26-406.

reasonably related to the value of the consumer's data.[444]

132 California Civil Code (CIV) § 1798.175 provides that in the event of a conflict, the law that provides the greatest privacy protection takes precedence. However, the CCPA appears to prevent some of these conflicts by clarifying that it neither applies to medical information governed by the Medical Information Act nor to protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued pursuant to HIPAA and the HITECH Act.[445] Further reservations concern the FCRA, the GLBA and the CFIPA.[446]

IV. Findings

133 All data processing operations in Switzerland and in the EU have to comply with applicable data protection law. Swiss data protection law makes the analysis of special (i.e. sensitive) categories of data subject to additional safeguards and the GDPR prohibits the processing of similar categories of data as a matter of principle. However, while both jurisdictions recognise a fundamental right to data protection, they also recognise that such right is by no means absolute. Hence, data processing in general, as well as profiling with the use of special categories of data in particular, is permitted with the data subject's consent. The main restriction here is that this consent has to be given freely and may be withdrawn without further ado. The processing of personal data for the personalisation of insurance contracts could also be deemed legitimate as far as it is necessary for the performance of such contracts or for pursuing a legitimate interest of the insurance company. In addition, insurance companies must ensure that their (potential) policyholders are aware that their personal data is processed to calculate individual offers based on their individual risk profile and/or their willingness to pay.

134 The restrictions these requirements impose on the individualisation of insurance contracts mainly depend on how the notions of "transparency", "freely given consent" and "legitimate interest" are understood. While there are convincing reasons to acknowledge that the lawfulness of processing personal data for offering individual insurance contracts can be based on the legitimate interests of insurance companies or should be considered compatible with the initial purpose of the insurance contract in most cases, it is hard to predict whether data protection authorities and courts would actually accept this reasoning. As a consequence, insurance companies are well advised to always ask for the specific consent of their (potential) policyholders prior to processing their data for providing an individual offer.

135 In California, a patchwork of privacy laws needs to be observed when individualising insurance contracts. Some federal laws set significant limits to individualisation based on certain categories of data, such as HIPAA's prohibition to disclose and GINA's prohibition to request or purchase genetic information for underwriting purposes. The majority of the rules, however, require transparency and security about data processing operations, without setting specific boundaries to individualisation. On the state level, most notably the IIPPA vests consumers not only with a right to have recorded information corrected or a portion of it deleted, but actually limits the informational basis for adverse action taken against the insured. The CFIPA also restricts information sharing between insurance companies and non-affiliates, but does not limit personalisation based on information in possession of the insurance or fully owned subsidiaries. While the novel CCPA will grant consumers the possibility to opt-out from having their information sold, the personalisation of insurance contracts appears to still be possible, since it is arguably reasonably related to the value of the consumer's data.

136 In sum, the all-encompassing Swiss and European approach to data protection law operates with very abstract concepts which leaves insurance companies with a great margin of interpretation and a remarkable amount of legal uncertainty. However, using big data analytics for the individualisation of insurance contracts is not prohibited by data protection law and should be compliant as long as the correct safeguards are in place, notably by requesting the data subject's consent. In California, data may be used for big data analytics in principle. But since rate increases qualify as adverse actions by statute under the IIPPA and the CCRAA, these regulations limit an insurer's informational basis. Thus, Californian data privacy laws set forth some significant and specific boundaries to the individualisation of insurance contracts.

444 CIV § 1798.125(a)(1); Determann (n 434) 120.

445 CIV § 1798.145(c)(1)(1). However, Determann states that the CCPA does not address any overlaps or inconsistencies with any of California's existing privacy laws (Determann (n 434) 117).

446 Ballon (n 432) 26-422.

F. Conclusion

137 The aim of this paper is to outline possible solutions for dealing with the individualisation of insurance contracts, namely with regard to individually calculated insurance premiums. It does so by analysing the legal situation on both sides of the Atlantic, using the jurisdictions of California and Switzerland as examples for two quite different approaches. The individualisation of insurance contracts has become technically possible and economically feasible in most insurance sectors thanks to novel technologies such as big data analytics. In order to provide a broad picture, this paper does not focus on one specific type of insurance, but includes three different types; namely, mandatory health insurance, renters insurance and automobile insurance. In addition, we analyse individualisation based on the two most important criteria in the insurance sector: individualisation based on the risk profile of the insured and individualisation with regard to his or her willingness to pay. Obviously, these two criteria can be combined when calculating the individual premium of a customer, but it seems that (until now) insurance companies have been rather reluctant to individualise their contracts according to their customers' willingness to pay.

138 Whether insurance companies should be allowed to individualise their contracts and premiums or whether the principle of solidarity should prevail, is being debated in various disciplines. While ethical considerations may speak in favour of solidarity at least for some types of insurance,[447] an economic analysis would reach the conclusion that the individualisation of insurance contracts is beneficial for most individuals and the society at large. Given these different perspectives and the importance of the respective arguments, there is certainly no simple answer on how to deal with the individualisation of insurance contracts. Accordingly, it may come as no surprise that the two jurisdictions we have chosen to analyse – Switzerland and California– do not only rely on very different approaches to deal with the phenomenon, but they also come to quite different conclusions. Perhaps surprisingly, the leeway for individualisation is much smaller in California than in Switzerland for renters and automobile insurance, while the results are very similar for mandatory health insurance.

139 In Switzerland, the insurance sector is regulated as well, but less densely than in California and there are also important variations between different types of insurance. While there is strictly no leeway for individualising mandatory health insurance contracts in Switzerland, an insurer is free to do so with regard to supplementary health insurance policies. As opposed to health insurance, renters and automobile insurance are generally governed by the principle of freedom of contract, thereby allowing almost unlimited choices to insurance companies. Although Switzerland prohibits discrimination on a constitutional level and also through the Civil Code as well as other regulations, anti-discrimination law does not restrict the ability to individualise insurance contracts as long as factoring in a protected characteristic such as age, gender and the like is based on a sound actuarial risk-assessment is based on a sound actuarial risk-assessment. The most important restrictions for the individualisation of insurance contracts stem from data protection law, from the Swiss Data Protection Act (DPA) as well as from the EU's General Data Protection Regulation (GDPR). These bodies of law contain important barriers for analysing personal data about the potential customers and the population at large. As a result, the individualisation of insurance contracts is only clearly allowed if the customer's specific consent is obtained, while justifying the individualisation with legitimate interests comes with considerable legal uncertainties.

140 In the U.S. and California, the insurance sector is densely regulated. Individualisation based on the willingness to pay is straight-forwardly excluded in California by way of a notice enacted by the Insurance Commissioner. The leeway to individualise offers based on the risk assessment of individual customers is very limited in all three insurance sectors considered. This is especially true for the comprehensively regulated health insurance market. While there is a little more leeway for the individualisation of automobile and renters insurance, the scope is still very limited as the rates for these types of insurance are subject to prior approval by the California Insurance Commissioner and the maximum and minimum permitted premium is determined by law. As a consequence, insurance law limits the ability of insurance companies to individualise their insurance contracts to a minimum. In addition, U.S. and California law contain strict rules with regard to anti-discrimination, which further restrict the remaining leeway if protected characteristics such as age, gender, race, or place of residence are factored into the calculation individual premiums. As a consequence, the leeway for the individualisation of insurance contracts in California is so small that it is doubtful whether running big data analytics to individualise insurance premiums is commercially feasible. As opposed to Switzerland and Europe, however, data privacy laws establish no relevant restrictions for the individualisation of insurance contracts in the U.S. and California.

447 Michele Loi and Markus Christen, 'Choosing how to discriminate: fair algorithms and risk prediction with big data in the insurance sector', unpublished manuscript.

141 Given the restrictions on both sides of the Atlantic and the potential benefits of the individualisation of insurance contracts, both on an individual and a societal level, the result of the analysis is hardly satisfying, especially with regard to Switzerland (and Europe). Instead of directly or indirectly hindering the individualisation of insurance contracts through data protection law, Swiss (and European) lawmakers should initiate a dialogue involving all stakeholders to determine which sectors of insurance should be dominated by the principle of solidarity and in which sectors the individualisation of insurance contracts should be allowed. It is to be expected that there will be no uniform answer for all types of insurances. Rather, there may be sectors in which solidarity should prevail to ensure that no one is excluded from insurance coverage; the most important case in point being mandatory health insurance. By contrast, automobile insurance might be a sector in which the individualisation of insurance contracts should be allowed to ensure the benefits of the incentives provided by individual premiums that are calculated based on individual risk profiles of very prudent or more hazardous drivers.

142 While this approach should be able to provide nuanced and convincing results, it is obvious that such a process will need time. For the time being, a meaningful step forward would be to allow for factoring in the public interest when assessing the lawfulness of processing of personal data based on the legitimate interest of the controller. This would allow insurance companies to at least use readily available data for calculating and offering individual insurance premiums. The consent of their customers would then only be needed if insurance companies wanted to collect additional data, e.g. on driving behaviour or the physical activity of their customers, by using driving or fitness trackers, or other means to collect additional data.

Acknowledgements

We would like to thank Joseph Lavitt, lecturer at Berkeley Law, University of Berkeley, California, for his very generous help with regard to all aspects of U.S. law; Prof. Paul Schwartz, Berkeley Law, University of Berkeley, California, for his valuable input; David O'Brien, Assistant Director of Research at the Berkman Klein Center for Internet and Society at Harvard University for his valuable comments on U.S. and California privacy law; and the staff at the California Department of Insurance for valuable input on various issues of California insurance law.

This research has been supported by the Swiss National Science Foundation as part of the project "Between Solidarity and Personalization – Dealing with Ethical and Legal Big Data Challenges in the Insurance Industry" (application no. 407540_167218/1). With the exception of some last minute developments, literature on U.S. and Californian law is updated until August 2018. Literature and case law on Swiss and European law has been considered until May 2019.