GLI GLOBAL LEGAL INSIGHTS

AI, Machine Learning & Big Data

2022

Fourth Edition

Contributing Editor: **Charles Kerrigan**

glg global legal group

Global Legal Insights
AI, Machine Learning & Big Data

2022, Fourth Edition
Contributing Editor: Charles Kerrigan
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – AI, MACHINE LEARNING & BIG DATA

2022, FOURTH EDITION

Contributing Editor
Charles Kerrigan, CMS Cameron McKenna Nabarro Olswang LLP

Publisher
James Strode

Production Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Charles Kerrigan of CMS Cameron McKenna Nabarro Olswang LLP for all of his assistance.

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

ISBN 978-1-83918-190-0
ISSN 2632-7120

Printed and bound by TJ Books Limited
Trecerus Industrial Estate, Padstow, Cornwall, PL28 8RW
May 2022

CONTENTS

Switzerland

Jürg Schneider, David Vasella & Anne-Sophie Morand
Walder Wyss Ltd.

Trends

According to various rankings, Switzerland has been considered the most innovative country worldwide over the past few years. In the European Innovation Scoreboard 2021 report, in which Switzerland is described as the "overall innovation leader in Europe", the European Commission noted that Switzerland's strengths lie in attractive research systems, human resources and intellectual assets. The top three indicators include international scientific co-publications, foreign doctoral students and lifelong learning. The annual report identifies the relative strengths and weaknesses of innovation systems in EU member countries, European countries outside the EU, and their regional neighbours. This is done based on four main indicators, for each of which Switzerland scored best:

- Framework conditions (dimensions of human resources, attractive research systems, and innovation-friendly environment).
- Investment (financing and support and business investment).
- Innovation activities (innovators, linkages and intellectual property).
- Impact (impact on employment and impact on turnover).

With regard to the topic of Artificial Intelligence (AI), Switzerland has the highest number of AI patents in relation to its population worldwide, and the highest number of AI companies per citizen in Europe. This makes Switzerland one of the leading centres for AI development. Additionally, the country has a large number of leading research institutes in the field of AI, such as the two Federal Institutes of Technology ETH Zurich and EPFL Lausanne. ETH Zurich in particular opened a new research centre for AI, the ETH AI Center, in 2020. This centre aims to intensify the interdisciplinary dialogue with business, politics and society on the innovative and trust-promoting further development of AI. This proximity to research and innovation is a decisive reason for global technology companies such as Google, IBM and HPE to use Switzerland as a research location. Due to its traditional strengths in life sciences, Switzerland is also driving AI development in the healthcare and pharmaceutical sectors. With a stable political and economic environment and globally operating companies, Switzerland offers a secure location for the storage, processing and validation of data. Furthermore, with International Geneva, Switzerland has a location that fulfils many of the requirements for becoming a centre for the global governance of AI. Geneva attracts many international organisations and standards organisations that are also centres of normative power, or may be considered as such. For instance, the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) are Geneva-based organisations. The ICO and IEC are even associations established under Swiss law. This potentially enables Switzerland, on an informal basis, to provide early input

into standards-setting in relation to AI. Hence, in principle, Switzerland is well positioned for the application and challenges of AI; however, the political environment has highlighted an additional need for action in various areas. To ensure that Switzerland remains one of the leading countries in the development and application of digital technologies, the Federal Council made AI a core theme of the Digital Switzerland Strategy in 2018 and set up an interdepartmental working group under the guidance of the State Secretariat for Education, Research and Innovation (see also the section "Regulations/Government intervention").

In addition, Switzerland is monitoring regulatory developments in the EU. On 21 April 2021, the European Commission published a proposal for an "Artificial Intelligence Act" – a draft bill on the regulation of AI – in order to develop human-centric AI and eliminate mistakes and biases to ensure AI is safe and trustworthy. The draft bill follows the European Commission's "White Paper on Artificial Intelligence" which was published on 19 February 2021 and represents the starting point for the regulation of AI in the EU. The draft bill extends far beyond the borders of the EU. The current draft bill will apply to all AI systems that are placed on the market in the EU or that affect people in the EU. Especially in the software sector, where new products are costly to develop but very cheap to reproduce, such rules can quickly have an impact in other countries, including Switzerland. Most AI providers will not develop their own products for Switzerland, hence new European standards will have an impact in Switzerland as well, as did the introduction of the European General Data Protection Regulation (GDPR) in 2018 (see also the section "Regulations/Government intervention").

On 13 April 2022, the Federal Department of Foreign Affairs (FDFA) published the "Artificial Intelligence and International Rules" report. In submitting this report, the FDFA had fulfilled a task assigned to it by the Federal Council. The report sets out various measures to allow Switzerland to play an active role in shaping and contributing to an appropriate global set of AI rules that addresses the challenges and exploits the opportunities presented by AI. The measures proposed to the Federal Council shall boost Switzerland's legal and technical expertise, ensure that its positions on AI are coherently represented in international bodies, and, by working with the Geneva-based international standards organisations, make an active contribution to shaping global AI rules and standards. According to the report, the proposed measures will also reinforce Geneva's profile as an international hub for digital issues.

Ownership/protection

AI systems, which are partly trained with data that are themselves subject to legal provisions as stipulated under Swiss intellectual property law, must be protected adequately. Furthermore, in certain circumstances, AI systems are also capable of creating "novelty" so that the question may arise of whether inventions created using AI may be protected by copyright or patents and if so, who is entitled to the rights thereto.

Patents

In Switzerland, the prevailing opinion is that only natural persons may be inventors in the sense of the Swiss Patents Act (PatA), which excludes the possibility of recognising AI systems as inventors due to their lack of legal capacity and legal personality. However, it is irrelevant how inventions are created and a subjective achievement of the inventor is not required. Pursuant to Article 1 paras 1 and 2 PatA, patents are granted for new inventions applicable in the industry, while anything that is obvious having regard to the state of the art is not patentable.

According to prevailing opinion in Switzerland, Swiss patent law recognises only natural persons as inventors in the legal sense. However, inventions created through or by AI can

be assigned to a natural person as an inventor and are thus, in principle, patentable. The natural person who first took note of the invention and understood it as a solution to a technical problem is usually considered the inventor of an AI-generated invention.

Copyright

According to Article 2 para. 1 Swiss Copyright Act (CopA), works that are considered an intellectual creation with individual character may be protected by copyright. Under the CopA, computer programs may also qualify as works and therefore enjoy copyright protection if they meet the legal requirements. It can be argued that AI algorithms as expressed in a certain programming language may be subsumed under the concept of a computer program and thus copyrightability of such AI may be affirmed. Although the CopA provides no legal definition for a computer program, it is commonly understood in a narrow sense so that AI may not be considered as a copyrightable work under the CopA after all. It may, however, be argued that the lack of a legal definition reflects the will of the Swiss legislator to leave room for future technological developments and new forms of potentially copyrightable computer programs which include or use AI. Furthermore – and similarly to Swiss patent law – pursuant to Article 6 CopA only natural persons may be authors of copyrightable works. If computers are used as tools of the author, a work may be attributed to the natural person who is controlling the AI-based process. However, if a work was autonomously created by a computer without any human control involved, copyrightability may be denied as the work is not considered attributable to a natural person. Where exactly the line should be drawn between AI as a simple tool and AI autonomously acting as an author (or rather creator) of the work is currently the subject of controversial debate. If, however, an intellectually creative relationship between the human programmer or operator of an AI and the AI-generated work no longer exists, there is a risk copyright protection will be denied under Swiss copyright law.

Furthermore, many AI applications require substantial amounts of data for their learning and training process such as e.g. photographs used for training image recognition software. As some of this data will regularly be protected by copyright and the gathered data will usually be reproduced for use by the AI application, this may constitute, if used without licence, a copyright infringement as stipulated in Article 10 para. 2 letter a CopA since the right to produce copies exclusively pertains to the author of the work. Swiss copyright law will therefore have to address this issue in view of the rapid development of AI systems heading towards more autonomy.

Antitrust/competition laws

Antitrust

The use of AI may be relevant under antitrust law if parameters relevant to competition, such as e.g. prices, are affected. In particular, price algorithms can be specifically programmed in such a way that prices agreed between competitors for online offers are not undercut or that they are used to implement signalling strategies. Further, price algorithms may promote behavioural coordination between competitors as market transparency is increased and the possibility of reacting more frequently and more quickly to price adjustments is thus extended. However, the Swiss Cartel Act (CartA) is worded in a technology-neutral manner and hence does not contain any specific provisions on the use or implementation of AI so that the general rules – as in particular the provisions on the prohibition of cartels – apply. If algorithms are used in a coordinated manner and with the intention of influencing the price as a competitive parameter, this may constitute a deliberate and

intentional interaction and thus an agreement affecting competition in accordance with Articles 4 paras 1 and 5 CartA. Moreover, price algorithms can potentially be relevant with regard to unlawful practices by dominant undertakings or undertakings with relative market power in accordance with Article 7 CartA. According to Article 7 CartA, a relative market power or dominant market position may not be abused by undertakings in order to hinder other undertakings from starting or continuing to compete or disadvantage trading partners. If a price algorithm is used to enforce unreasonable prices or terms and conditions and provided other undertakings are hindered from starting or continuing to compete or concerned undertakings are disadvantaged and there is no justification for such behaviour, the latter may qualify as unlawful under the CartA.

Unfair competition law

If false or misleading information affects competition, the Swiss Act against Unfair Competition (UCA) applies. The purpose of the UCA is to enable providers, customers, trade associations and consumer protection organisations to take legal action against the dissemination of market-relevant disinformation. If consumers' purchase decisions are manipulated in a legally relevant matter by means of, e.g., recommendation algorithms or other AI applications, there is a risk that consumers may invoke the provisions as stipulated in the UCA. However, currently there is hardly any pertinent case law in Switzerland regarding such manipulation so that it is unclear when courts would rule the latter to be legally relevant. For AI applications, such as, e.g., personalised prices or advertising, it is argued that a legally relevant manipulation under the UCA is likely to be denied, whereas it cannot be excluded that the situation could be viewed differently in cases where the decision-making is modelled in such a way that consumers appear to have no actual choice. Furthermore, the legal situation is unclear at present regarding situations where AI applications lead to non-market-relevant manipulations. In any case, further development of the law including upcoming relevant core practice will have to be closely monitored to identify potential future distinction between user manipulation by means of AI applications that is considered acceptable under the current law on the one hand and legally relevant and therefore problematic on the other hand.

Board of directors/governance

According to the Swiss Code of Obligations (CO), the board of directors of a Ltd. either manages the business itself or assigns responsibility for management to a third party. If assignable tasks are given to third parties, the board of directors of a Ltd. is only liable for the selection, instruction, and supervision of the representatives. However, according to Article 716a CO, the board of directors has seven non-transferable and inalienable duties, including the overall management of the company and the issuing of all necessary directives, the determination of the company's overall organisation as well as the organisation of the accounting, financial control and financial planning systems as required for general management of the company. In Switzerland, there are currently no AI-specific guidelines with which a board of directors must comply. However, when addressing the topic of corporate governance, Swiss companies often follow the "Swiss Code of Good Practice for Corporate Governance", a guide published by *EconomieSuisse*, the umbrella association of Swiss companies, and the corporate governance directives of *Six Swiss Exchange*, the Swiss stock exchange.

Under the keyword "digital board member", the use of AI in boards of directors has recently been discussed more frequently. For activities that require a high degree of rationality and

data-driven decision-making, a future use of AI is quite realistic. AI can help to optimise decision-making processes, rendering decisions based on data-backed knowledge and better predicting of the impact of such decisions possible. There is currently no obligation under Swiss law to include AI in board decisions, but it remains to be seen whether an obligation to use AI can be derived from the board's due diligence in the future (see also the section "Civil liability"). It may therefore be worthwhile for a board of directors to already analyse the benefits that AI could bring in the area of corporate governance. The use of AI can be seen as an extension of the board's competences and can generate enormous benefits. The advantages made possible by the selective use of AI, if identified early, can be a crucial competitive advantage. It is advised that the responsible board of directors follows this trend.

Regulations/government intervention

In 2018 the Federal Council made AI a core theme of the so-called "Digital Switzerland Strategy", a strategy on digital policy, which is complemented by further sectoral strategies. The strategy is relevant for the actions taken by the Federal Administration and can serve as a framework for other Digital Switzerland stakeholder groups such as the scientific and business community, the administrative authorities and also the civil society. As part of the strategy, an interdepartmental working group on AI was set up. In December 2019, the group published a report in which the AI challenges Switzerland may face are explained. The report stated that relevant legal principles in Switzerland would usually be worded in a technology-neutral way so that they could also be applied to AI systems. It was specifically pointed out that the existing legal framework would already permit and regulate the use of AI in principle (e.g. Federal Act on Gender Equality), and apply in particular to discrimination that may arise as a result of AI decisions (see also the section "Discrimination and bias"). Thus, in summary, for the moment, there is no need for fundamental adjustments to the legal framework. In 2020, the same interdepartmental working group then developed guidelines on the use of AI within the Federal Administration, meaning a general frame of reference for federal agencies and external partners entrusted with governmental tasks. The guidelines were adopted by the Federal Council in November 2020.

In 2021, the Federal Council indicated that the relevant developments regarding the European regulation of digitalisation and their impact on Switzerland would be closely monitored in order to be able to take measures at an early stage if necessary. It may be noted that the further development of the EU's draft AI Act will increasingly influence political processes and debates about the topic of AI regulation in Switzerland. Switzerland will inevitably have to position itself on the topic – firstly, because research and politics are increasingly calling for the adoption of framework conditions for the reasonable use of AI. Secondly, Switzerland is shaped by EU legislation, as it is closely linked to the EU internal market and therefore dependent on (EU) market access. Although this does not necessarily mean that Switzerland must follow the EU rules, when the AI Act is going to enter into force (probably in 2024), the need for action will in any case intensify. A reflective and evidence-based debate on how the use of AI should be shaped in Switzerland is thus to be expected – especially because a high number of AI companies are based in Switzerland (see also the "Trends" section).

Civil liability

A crucial challenge regarding the use of AI is civil liability in the event of damage. Even though the general provisions on liability, as stipulated in the Swiss Code of Obligations

(CO), also apply to AI systems, proving that the respective prerequisites for liability are met is associated with difficulties, particularly concerning the proof of fault. Certain areas of law have provisions on liability that apply to AI systems as well, such as e.g. for autonomous vehicles in the Swiss Road Traffic Act (RTA) or for autonomous drones in the Swiss Air Traffic Act. If, for instance, an autonomous vehicle causes an accident due to a faulty object detection, questions on who or what is liable for the damages incurred arise. While it is the human controlling a "regular" vehicle who is responsible for object detection and collision avoidance, it is the AI system which takes over control in the case of an autonomous vehicle. In any case, under current Swiss law, the owner of the vehicle is subject to civil liability pursuant to Article 58 RTA, irrespective of the nature of the vehicle. Furthermore, it increasingly becomes apparent that in the future the focus of civil liability in Switzerland will be on the manufacturer of AI systems. In that respect and with certain adjustments to be made, the Swiss Product Liability Act (PLA) could gain importance in view of future technological developments for AI systems.

Swiss product liability law in its current state does not fit AI applications well, especially when it comes to determining the product nature of software, inaccuracy of decisions or aftermarket obligations of the manufacturer. Additionally, the role of the manufacturer is changing in light of the variety of persons influencing the design, functioning and use of AI systems.

According to the prevailing doctrine in Switzerland, software may be qualified as a product in accordance with the PLA as it can create product-typical risks of damage so that liability as derived from the PLA may be applied to AI applications as well. The standards for determining defectiveness of AI applications need, however, to be clarified under Swiss law, especially since many AI systems are self-learning, constantly evolving and thus potentially beyond the manufacturer's sphere of responsibility. According to Article 4 PLA, a product's defectiveness is assumed if it does not offer the safety that may be expected considering all circumstances at the time the product is first placed on the market. Pursuant to Article 5 PLA, there is no liability for defects that only arise after the product was placed on the market. This may give rise to issues especially considering that some AI applications are self-learning and adapting to their environment. This means that in certain cases AI systems may develop new and independent solutions only after first being put on the market so that liability for such later and potentially erroneous modifications would be excluded under the current legal system. In principle, the manufacturer of an AI application is supposed to minimise the potential risks emanating from the AI through careful programming and training. However, where self-training and self-learning AI applications are concerned, the control of the manufacturer is reduced substantially. On the other hand, users of the AI may be able to influence an AI system by selecting the learning method or the duration of the learning process as well as the training data. It may hence be argued that users may be liable if their influence leads the AI to a faulty decision that causes damage so that manufacturers may exonerate themselves due to the improper influence of third parties. Again, it might prove helpful to clarify these uncertainties in terms of liability with an amendment of the current legal framework.

Under Swiss contract law, the obligor is liable for any intentional or negligent breach of contract. Accordingly, if an AI application causes a breach of contract, the operator may be liable in case of intentional or negligent use. Interestingly, it is debated whether if the use of an AI system in a specific field of service is established, such use of an AI application may in the future constitute the minimal standard for diligently provided services.

At present, various new forms of legal basis of liability for AI systems are discussed such as, e.g., applying existing liability provisions by analogy, the introduction and implementation of further sector-specific liability clauses distinguishing between the manufacturing and the use of AI applications or the introduction and implementation of provisions for liability of AI systems specifically.

Criminal issues

Swiss criminal law is technology-neutral and the Swiss Criminal Code (CrC) does not provide any specific provisions regarding criminally relevant behaviour of AI systems. According to the general principles under Swiss criminal law, the personal culpability of the offender is required. However, the possibility of AI applications acting culpably is currently denied, as they have neither legal capacity nor legal personality. Thus, criminal liability must necessarily be attributed to either the manufacturer, programmer or operator of an AI application.

If an AI system carries out an action that qualifies as a criminal act under the CrC, the question of who is responsible or what caused the AI system's criminally relevant action arises. If the cause of action lies in faulty programming, this may constitute a negligent act of the programmer or manufacturer. However, in case of negligence, the CrC must explicitly state that the negligent act is punishable for the specific offence. Further, in case of negligence, there must be a violation of duty of care that led to or caused the punishable offence and it must have been foreseeable for the offender that the adopted behaviour would lead to the punishable offence. However, the foreseeability on the side of the offender may be hard to assume if the AI application concerned operates rather autonomously and especially if it is self-learning and adaptive. Hence, it may be questionable if the evolved behaviour of the AI system is still attributable to the manufacturer, programmer or operator. Moreover, if the concerned AI application was deliberately programmed to induce the criminal act, manufacturers, programmers or operators may be viewed as having acted intentionally (this may be relevant with regard to misuse of military equipment such as drones or in terms of cybersecurity, for instance, when it comes to hacking robots). In a case where the AI application was programmed correctly but used improperly, the operator or user may be criminally liable.

A fairly recent trend shows that AI systems may be implemented as tools for so-called Predictive Policing and crime prevention, which rely on big data, AI algorithms and the evaluation of the same. Predictive Policing encompasses predictions about the occurred crime itself and the crime location, predictions about the victim(s), predictions about an individual's potential delinquency and predictions about the criminal profile of the offender(s). The aim of Predictive Policing is the evaluation of existing data and a gain in knowledge which ultimately allows for estimations or assessments on the crime and at best for prevention of future crimes. Nonetheless, as AI algorithms are unlikely to ever be completely neutral or unbiased, Predictive Policing may lead to problematic or even discriminatory assumptions based on the collected and combined data. As this is a new concept, in Switzerland there is a lack of clarity on its implementation and handling. What is required in the future is therefore a comprehensive definition of the scope and specific application necessary.

Discrimination and bias

Data protection – Automated individual decision-making

In a growing number of areas of life, technological advances – especially in the field of AI or machine learning – are leading to an increase in automated decisions based on algorithms. A practical example is the automated decision in an application procedure or an automated

termination of a contract. In Switzerland, automated decisions are not specifically regulated under the current FADP (in contrast to the GDPR). This will change with the entry into force of the revised Federal Data Protection Act (FADP). The amended FADP was adopted by the Swiss Parliament on 25 September 2020, and its entry into force is expected to occur on 1 September 2023. The new FADP will contain a provision for decisions that are taken exclusively on the basis of automated processing. The provision obliges the data controller to inform data subjects of automated individual decisions that have legal effects on the data subjects or affect them significantly (unless exceptions apply). Although the substantive content is similar to that of the GDPR, the Swiss provision is based on a completely different concept: the new provision in the revised FADP is merely a duty of information and not a prohibition as in the GDPR. If the requirements of the duty of information are met, data subjects have the possibility to state their position upon request. Data subjects may also request that such decision be reviewed by a natural person, for example, because the data subjects suspect that they have been disadvantaged by an AI due to bias. However, there is no possibility for data subjects to challenge the decision, as is the case under the GDPR.

Transparency is important for the users of AI applications in order to be able to understand with which data an algorithm has been trained and how the algorithm is constructed. The draft EU AI Act specifies under the provisions on transparency requirements for high-risk AI systems what is required in the GDPR regarding the disclosure of logic in automated decision-making. Such a specification is missing under Swiss law – although the revised FADP explicitly states within the provision on access rights that data subjects must be informed about the logic on which the decision is based; however, it does not say anything about how the logic of automated decisions must be disclosed. It may be argued that a company will not be obliged to provide a detailed explanation of the algorithms used or to disclose the entire algorithm. Nevertheless, the information provided should be comprehensive enough to allow data subjects to understand the reasons behind the decision.

For this reason, companies are advised to develop simple procedures to inform the data subjects concerned about the underlying considerations and criteria of the automated individual decisions. For this purpose, it would be sensible to implement an appropriate internal process and to analyse the AI application to be used well in advance.

Bias by AI in the context of employment

There is no general anti-discrimination law in Switzerland. However, under Swiss labour law, there is a general principle of non-discrimination that is derived from the concept of protection of personality as stipulated in Article 328 Swiss Code of Obligations (CO). A discriminatory violation of personality exists if the unequal treatment of an employee is linked to personality traits that are sensitive to discrimination. Pursuant to Article 328 CO, AI applications in the employment context must not be programmed in such a way that they discriminate directly nor indirectly, i.e. have a discriminatory effect on different groups of employees (based on age, gender, race, nationality, etc.) despite neutral programming, unless such application is objectively justified and proportionate. The general principle of non-discrimination under labour law is complemented by other principles of non-discrimination based on special legislation. Those are the following:

(1) direct and indirect discrimination linked to gender is prohibited under the Swiss Gender Equality Act (GEA);
(2) the Swiss Disability Discrimination Act (DDA) stipulates the principle of non-discrimination for disabled people, although it only applies to federal employment contracts and not employment under private law;

(3) the Swiss Act on Human Genetic Testing (HGTA) provides protection from genetic discrimination; and
(4) the Agreement of Free Movement of Persons between the EU and Switzerland prohibits discrimination of European migrant workers with regard to recruitment, employment and working conditions.

An AI application commonly used in employment consists of the so-called "People Analytics" (forming part of "Predictive Analytics"), which helps employers identify, hire, retain and reward their employees via data analysis. This is done with the help of algorithms that aim to slice and dice a large amount of data to extract specific information on employees. The so-called Big Data collected during this process and the AI systems used can then combine previously unrelated data to make accurate predictions via Predictive Analytics. Further, machine learning models are used to identify trends, patterns and relationships between the gathered data of employees. On the basis of the patterns discovered, things and activities will be classified, their value estimated and behaviour will be predicted based on probabilities. The goal of Predictive Analytics is to provide a foundation for attributing certain characteristics to an individual employee that are linked to other employees who appear statistically similar. Within the same process, those employees who appear statistically different will be separated from the rest so that a (statistical) discrimination may occur. Discrimination can be related to the input data, the analysis model or the output of the applied AI application.

While AI may help employers optimise operations in their business, the AI applications used may (involuntarily) discriminate employees. However, certain legal authors argue that the currently applicable legislation which offers protection against employee discrimination does not (sufficiently) cover discrimination by AI applications due to the difficulty of proving its existence and due to the lack of deterrent sanctions when violating the applicable law.

National security and military

Switzerland is considered a hub of sorts in terms of cybersecurity with different notable actors promoting cooperation and interaction in this field. In 2019, the so-called Cyber-Defence Campus was founded where governmental, academic and industrial actors interact and which focuses on various matters of national defence also with regard to cybersecurity. As the Swiss government detected a lack of clear policy in respect of cybersecurity, it adopted in 2018 a national strategy for the protection of Switzerland against cyber-risks (the so-called NCS) with the aim of implementing a broad set of measures. The NCS also led to the creation of a centralised cybersecurity body on a federal level, the National Cyber Security Centre, which, amongst other tasks, serves as a contact point for market actors. The NCS further had an impact on federal laws, particularly in bolstering governmental powers in respect of intelligence services. However, there is currently no overarching and interdisciplinary cybersecurity act nor any political agenda of adopting such regulation.

Hence, Swiss data protection legislation often remains the starting point for any assessment of cybersecurity practices. The revised Swiss Act on Data Protection (FADP) calls for state-of-the-art data security measures without specifying technical standards, just like its predecessor which will be in force until the end of August 2023. The revised FADP thus maintains a future-proof and technologically neutral design. It is expected that the relevant ordinances to the FADP, which are currently being revised in view of the revised FADP, will provide more detailed information on proper data security measures and practices. Additionally, the revised FADP will introduce a duty to report, in certain circumstances,

data breaches to the competent data protection authority (the Federal Data Protection and Information Commissioner, FDPIC) or even the data subjects directly. Moreover, the Swiss government plans to introduce a notification obligation for operators of critical infrastructures that are victims of a cyber-attack. It is important to note that under the revised FADP, individuals who intentionally failed to comply with the minimum data security requirements may face criminal fines of up to CHF 250,000. Thus, the criminal fines are not imposed on the company but on the person responsible for the data protection violation. However, under the revised FADP, companies may also be criminally fined with up to CHF 50,000 if an investigation on determining the responsible natural person within the company or organisation would entail disproportionate efforts. The offending persons are fined by the state prosecutors of the Cantons tasked with the enforcement of the FADP's criminal law provisions. The criminal fines are expected to work as a strong incentive for businesses or their responsible managers to ensure state-of-the-art cybersecurity.

Lastly, it should also be noted that governmental authorities such as Swiss criminal prosecution authorities or the Federal Intelligence Service have considerable legal competences when it comes to telecommunications surveillance and are permitted to penetrate protected systems for national security purposes under certain circumstances.

Jürg Schneider
Tel: +41 58 658 55 71 / Email: juerg.schneider@walderwyss.com

Jürg Schneider is a partner and co-head of Walder Wyss' data protection team and head of the Lausanne office. His practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. Jürg Schneider's special competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of the GDPR (and the upcoming revised Swiss FADP) for Swiss and international companies, and advising clients in regulated sectors (banking, insurance, healthcare, etc.) on data protection requirements.

David Vasella
Tel: +41 58 658 52 87 / Email: david.vasella@walderwyss.com

David Vasella is a partner and co-head of Walder Wyss' regulated markets, competition, tech and IP team. David Vasella advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. He deals with cross-jurisdictional data protection projects, including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. David Vasella also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, he frequently speaks and publishes in his areas of expertise. He is an editor of the Swiss journal for data law and information security and a member of the professional bodies International Association of Privacy Professionals (IAPP) and DGRI.

Anne-Sophie Morand
Tel: +41 58 658 56 34 / Email: anne-sophie.morand@walderwyss.com

Anne-Sophie Morand is an associate in the Regulated Markets, Competition, Technology and IP team at Walder Wyss. She advises on all aspects of data protection, information and technology law. Prior to joining Walder Wyss, Anne-Sophie Morand worked for the Swiss Data Protection Authority and the Swiss Parliament, and as a research assistant at the University of Lucerne. She obtained a Ph.D. with a thesis in the field of personal rights and sports sponsorship. She regularly publishes and lectures in her fields of expertise.

Walder Wyss Ltd.

Seefeldstrasse 123, P.O. Box, 8034 Zurich, Switzerland
Tel: +41 58 658 58 58 / URL: www.walderwyss.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

Banking Regulation
Blockchain & Cryptocurrency
Bribery & Corruption
Cartels
Corporate Tax
Employment & Labour Law
Energy
Fintech
Fund Finance
Initial Public Offerings
International Arbitration
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Pricing & Reimbursement

GLI GLOBAL LEGAL INSIGHTS