



# AI, Machine Learning & Big Data 2026

Eighth Edition

Contributing Editor:  
**Charles Kerrigan**  
CMS LLP

**glg** Global Legal Group

# TABLE OF CONTENTS

## Preface

**Charles Kerrigan**  
CMS LLP

## Expert Analysis Chapters

- 1**      **The regulation of AI in financial services: a review of the UK and EU position for firms developing AI products**  
**Lisa McClory**  
CMS LLP
- 9**      **Practical guidelines for the use of generative AI**  
**David V. Sanker**  
SankerIP
- 20**     **AI M&A: Current trends and unique legal and regulatory considerations**  
**F. Dario de Martino, Alex Touma, Anna Rudawski & Noah Brumfield**  
A&O Shearman
- 34**     **AI procurement**  
**Roch Glowacki, James Gill & Paul Caddy**  
Lewis Silkin LLP

## Jurisdiction Chapters

- 47**     **Argentina**  
**Diego Fernández**  
Marval O'Farrell Mairal
- 57**     **Cyprus**  
**Christiana Aristidou & Evdokia Marcou**  
The Hybrid LawTech Firm, empowered by Christiana Aristidou LLC
- 67**     **Finland**  
**Erkko Korhonen, Noora Wallenius, Taneli Lehtipuu & Joonas Ylä-Rautio**  
Borenius Attorneys Ltd
- 81**     **France**  
**Boriana Guimberteau & Elise Dufour**  
Stephenson Harwood
- 96**     **Greece**  
**Marios D. Sioufas**  
Sioufas & Associates Law Firm
- 114**   **Hungary**  
**Endre Várady, János Tamás Varga & Andrea Belényi**  
VJT & Partners

- 124 India**  
**Divjyot Singh, Riddhi Rahi, Shrishti Sharma & Tushar Todt**  
Alaya Legal
- 136 Indonesia**  
**Abadi Abi Tisnadisastra, Prayoga Mokoginta & Aloysius Andrew Jonathan**  
ATD Law in association with Mori Hamada
- 147 Ireland**  
**Victor Timon & Georgina Parkinson**  
Byrne Wallace Shields LLP
- 160 Japan**  
**Akira Matsuda & Ryohei Kudo**  
Iwata Godo
- 172 Kazakhstan**  
**Zafar F. Vakhidov & Zhanibek Nurgali**  
Vakhidov & Partners LLP
- 184 Lithuania**  
**Asta Macijauskienė, Renata Jankauskytė & Viktorija Stančikė**  
WIDEN
- 191 Malta**  
**Ron Galea Cavallazzi, Alexia Valenzia & Veronica Campbell**  
Camilleri Preziosi
- 202 North Macedonia**  
**Veton Goku, Ljupka Noveska Andonova, Martina Anđelković Apostoloska & Anisija Stojkowska**  
Goku & Partners in cooperation with Karanovic & Partners
- 210 Poland**  
**Monika Maćkowska-Morytz, Robert Brodzik, Jarosław Fejdasz & Wiktoria Ostrowidzka**  
Kochański & Partners
- 221 Singapore**  
**Lim Chong Kin, Anastasia Su-Anne Chen & Cheryl Seah**  
Drew & Napier LLC
- 235 Switzerland**  
**Jürg Schneider, David Vasella & Yannick Caballero Cuevas**  
Walder Wyss Ltd.
- 246 Taiwan**  
**Robin Chang & Eddie Hsiung**  
Lee and Li, Attorneys-at-Law

**257 Thailand**

**John Formichella, Naytiwut Jamallsawat & Onnicha Khongthon**

Formichella & Sritawat Attorneys at Law Co., Ltd.

**262 Ukraine**

**Yaroslav Baienko, Oleksandr Melnyk & Ivan Komar**

GOLAW

**280 United Kingdom**

**Charles Kerrigan, Erica Stanford, Lisa McClory & Ben Hitchens**

CMS LLP

**294 USA**

**Jon Polenberg, Alyssa Weiss, Gabrielle O. Sliwka & Rayaan A. Hossain**

Becker & Poliakoff

# Switzerland

**Jürg Schneider**

**David Vasella**

**Yannick Caballero Cuevas**

**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 2025 report, in which Switzerland is described as the most innovative country in Europe by exceeding the EU average innovation performance by 139.8%, the top six performance indicators include public–private co-publications, international scientific co-publications, foreign doctorate students, population involved in lifelong learning, job-to-job mobility of Human Resources in Science & Technology, and resource productivity.

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 AI research institutes, such as the two Federal Institutes of Technology: ETH Zurich; and EPFL Lausanne. ETH Zurich, in particular, opened a new research centre for AI in 2020, the ETH AI Center. This centre aims to intensify the interdisciplinary dialogue between business, politics and society on the innovative and trust-promoting development of AI systems. This proximity to research and innovation is a decisive factor for global technology companies, such as Google, IBM, OpenAI 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 ISO 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 Swiss Federal Council made AI a core theme of the Digital Switzerland Strategy in 2018 already. Moreover, it set up an interdepartmental working group under the guidance of the State Secretariat for Education, Research and Innovation (see also the “Regulations/government intervention” section).

In addition, Switzerland continues to monitor regulatory developments in the EU, in particular the application of the EU’s Artificial Intelligence Act (AI Act). The AI Act applies to all AI systems that are placed on the market in the EU/EEA or that affect people in the EU/EEA. 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, much like the introduction of the European General Data Protection Regulation (GDPR) did in 2018.

In November 2023, the Swiss Federal Council instructed the Federal Department of the Environment, Transport, Energy and Communications (DETEC) and the Federal Department of Foreign Affairs (FDFA) to prepare an overview of possible regulatory approaches to AI that build on existing Swiss law and are compatible with the AI Act and the Council of Europe’s AI Convention (AI Convention). Consequently, on 12 February 2025, a report was presented to the Swiss Federal Council outlining the possible regulatory approaches to AI. On the basis of this overview, the Swiss Federal Council has decided on an approach based on three objectives: strengthening Switzerland as a location for innovation; safeguarding the protection of fundamental rights, including economic freedom; and increasing public trust in AI. To achieve these objectives, the Swiss Federal Council has set the following key steps for the future:

- the AI Convention will be integrated into Swiss law, primarily applying to state actors;
- where legislative amendments are necessary, they will be sector-specific whenever possible; in general, cross-sectoral regulations will remain limited to areas relevant to fundamental rights, such as data protection; and
- beyond legislation, non-binding measures will be introduced, including self-disclosure agreements and industry-led solutions.

On 27 March 2025, Switzerland signed the AI Convention. The DETEC, together with the FDFA and the Federal Department of Justice and Police, is to prepare a draft bill for consultation by the end of 2026. The draft bill will define the necessary legal measures, in particular in the areas of transparency, data protection, non-discrimination and supervision, which are to be taken to implement the AI Convention. Additionally, by the end of 2026, these federal departments will also have to draw up a plan for non-legislative measures in order to take into account the rapid development of AI and to ensure that the Swiss approach aligns with that of its key trading partners. It is difficult to gauge – at this stage – when changes will effectively be incorporated into Swiss law and when non-legislative measures will be implemented. Finally, an advisory committee composed of representatives from political, economic, scientific and social circles has been established to discuss the measures required for the implementation of the AI Convention. At a session held in February 2026, Federal Councillor Albert Rösti emphasised that public trust in AI depended on such systems being transparent and intelligible.

## 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 questions may arise as to whether inventions created with AI technology 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 accordance with 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(1) and (2) PatA, patents are granted for new inventions applicable in the industry, whereas anything that is deemed obvious based on the current state of knowledge cannot be eligible for patent protection.

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.

Since 2016, patent applications for AI-based inventions have been growing exponentially, without indicating significant challenges. This suggests that the system is operating effectively and that there is currently no need for additional regulation in this area.

## Copyright

According to Article 2(1) of the Swiss Copyright Act (CopA), works that are considered an intellectual creation with individual character may be protected by copyright. Pursuant to Article 2(3) 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 that 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 AI and the AI-generated work no longer exists, there is a risk that 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 photographs used for training image-recognition software. As some of these 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 a licence, a copyright infringement as stipulated in Article 10(2)(a) CopA, since the right to create 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

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 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 – 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(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. Pursuant 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 discern potential future differences between user manipulation facilitated by AI applications that are deemed permissible under current laws and those that are legally significant and therefore problematic. Finally, it is worth noting that companies must also exercise caution when promoting AI-enhanced products. If their statements on products prove to be false or misleading, they may be accused of misleading their customers. This issue is commonly referred to as *AI washing*.

### Board of directors/governance

According to the Swiss Code of Obligations (CO), a company limited by shares (Ltd)'s board of directors is responsible for either managing the business itself or assigning the responsibility of 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 non-transferable and inalienable duties. These include 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 the company's general management. 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 “Directive on Information relating to Corporate Governance” by Six Swiss Exchange, the Swiss stock exchange. Even if not necessarily required, more and more boards of directors choose to appoint a committee from their members in the area of digitalisation/technology, including use of AI. This committee is tasked with ensuring that the full board of directors is provided with comprehensive information in the area of digitalisation/technology and AI.

Furthermore, under the keywords “digital board member”, the use of AI in boards of directors has recently been discussed more frequently. It is highly plausible that AI will be used in activities that require a high degree of rationality and data-driven decision-making. By providing data-supported insights and improving the prediction of outcomes, AI has the potential to enhance decision-making processes, enabling decisions to be based on knowledge backed by data, and allowing for better prediction of the impact of such decisions. 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 “Civil liability” section). 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 responsible boards of directors follow this trend.

## Regulations/government intervention

In 2018, the Swiss 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 civil society. As part of the strategy, an interdepartmental working group on AI was established. 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 “Discrimination and bias” section). Thus, in summary, at that time, there was 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 Swiss Federal Council in November 2020.

The “Digital Switzerland Strategy” sets guidelines for Switzerland’s digital transformation. The federal administration is obliged to adhere to it, while it also serves as a guiding principle for stakeholders involved in digitalisation. Switzerland wishes to prioritise digital offerings for the benefit of all citizens (digital first). Every year, the Swiss Federal Council determines some key topics as “focus themes” – these serve as a starting point for new measures and for Swiss Federal Council mandates. The three focus themes of 2025 are the implementation of the approach chosen by the Swiss Federal Council for regulating AI (as mentioned in the “Trends” section), the reinforcement of information security and cybersecurity for the whole of Switzerland, and the promotion of the use of Open Source Software in the federal administration. Since 2021, the Swiss Federal Council has been closely monitoring the development of European digital regulations, particularly the AI Act as well as the AI Convention, which have had a considerable impact on AI policy discussions in Switzerland.

As mentioned above (see also the “Trends” section), on 12 February 2025, the DETEC presented a report outlining possible AI regulatory approaches. Based on this report, the Swiss Federal Council adopted a strategy centred on three objectives: strengthening Switzerland as an innovation hub; safeguarding the protection of fundamental rights, including economic freedom; and increasing public trust in AI. To achieve these objectives, the Swiss Federal Council has decided to focus on the following parameters: the incorporation of the AI Convention into Swiss law; a sector-specific legislation as far as required; and the development of non-legally binding measures to support AI governance. By the end of 2026, the DETEC, FDFA and the Federal Department of Justice and Police will prepare a bill specifying the legal measures required for the implementation of the AI Convention, as well as a plan for non-legislative measures to reinforce the compatibility of the Swiss approach with that of its main trading partners. It is difficult to gauge – at this stage – when changes will effectively be incorporated into Swiss law and when non-legislative measures will be implemented.

## 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 CO, also apply to AI systems, proving that the respective prerequisites for liability are met poses challenges, particularly with regard to the proof of fault. Certain areas of law have provisions on civil liability that apply to AI systems as well, such as for autonomous vehicles in the Swiss Road Traffic Act (RTA).

Article 58 RTA establishes a strict liability for vehicle holders, making them liable for damage resulting from the use of their vehicle, irrespective of any fault on their part, unless an exception applies on the basis of Article 59(1) RTA. The latter allows vehicle holders to be released from civil liability if they can demonstrate that the damaging event was caused by *force majeure* or gross negligence on the part of the injured party or a third party, without any fault on the drivers’ or on the vehicle holders’ part or on the part of the persons for whom the vehicle holders are responsible, and without any defect in the vehicle having contributed to the damaging event. As a consequence, vehicle holders are not exonerated from their civil liability in case they or the drivers have been at fault. Similarly, when the vehicle’s driver assistance system is defective (even in the absence of fault on the vehicle holders’ or the drivers’ part), vehicle holders are not released from civil liability. Indeed, as the assistance system is integrated into the vehicle, the defect in this system becomes a defect in the vehicle. Such defects are attributable to the vehicle holders, even in the absence of any fault on their part or on the part of the drivers.

Furthermore, it is becoming increasingly apparent that in the future, the focus of civil liability in Switzerland will be on the manufacturers 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 manufacturers. Additionally, the role of the manufacturers is changing in light of the variety of persons influencing the design, functioning, and use of AI systems.

In accordance with the prevailing doctrine in Switzerland, software may be classified as a product under the PLA, as it can create risks of damage typical of a product. As a result, liability derived from the PLA may also be applicable to AI applications. 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 manufacturers’ sphere of responsibility. According to Article 4(1) 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(1)(b) PLA, there is no liability for defects that only arise after the product was placed on the market. This may give rise to certain 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, manufacturers of AI applications are supposed to minimise the potential risks emanating from AI through careful programming and training. However, where self-training and self-learning AI applications are concerned, control of manufacturers is reduced substantially. On the other hand, users of 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 might hence be argued that users may be liable if their influence leads AI to a faulty decision that causes damage; so, 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. A point of debate is whether the use of an AI system in a particular field of service, once established, may eventually become the minimum 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, personal culpability of the offender is required. As it currently stands, the ability of AI applications to act culpably is not recognised as they lack legal capacity and personality. Consequently, and as regards criminal liability relating to AI systems, only individuals with personal culpability could potentially engage their criminal liability.

As a noteworthy legislative development, the revised RTA now includes Articles 25a–25h, which specifically address the topic of automated vehicles. Article 25b(1) grants the Swiss Federal Council the authority to determine, by ordinance, the conditions under which a driver of an automated vehicle is exempt from their duty of control of the vehicle. Once implemented, these regulations will enable partial or full delegation of vehicle control to automation systems, thereby relieving the driver of criminal liability.

Moreover, a 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 that ultimately allows for estimations or assessments on the crime and at best 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, there is a lack of clarity in Switzerland on its implementation and handling. What is required in the future is therefore a comprehensive definition of the scope and specific applications.

## 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 specifically regulated under the Federal Data Protection Act (FADP). In fact, according to Article 21(1) FADP and unless an exception applies, the controller shall inform the data subject about any decision that is based exclusively on automated processing and that has a legal consequence for or a considerable adverse effect on the data subject (automated individual decision). Although the content is somewhat similar to that of the GDPR, the Swiss provision is based on a completely different concept; Article 21 FADP is merely a duty of information and not a prohibition as in Article 22 GDPR. Also, even if, according to Article 21(2) FADP, data subjects have the possibility to state their point of view as regards an automated individual decision and may also request that such decision be reviewed by a natural person, contrary to Article 22 GDPR, Article 21 FADP does not as such allow data subjects to challenge the automated individual decision. Furthermore, Article 21 FADP does not explicitly specify in which level of detail the logic of automated decisions must be disclosed to data subjects. It is sufficient that the information provided is comprehensive enough to allow data subjects to understand the reasons behind the automated individual decision. Neither a detailed explanation of the algorithms used nor a disclosure of the algorithm as such are required.

This being said, companies are well advised to implement appropriate internal processes to analyse any AI applications before use and to develop simple procedures to inform the data subjects concerned about the underlying considerations and criteria of their automated individual decisions.

### 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 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 or 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. These are the following:

- (1) direct and indirect discrimination linked to gender is prohibited under the Swiss Gender Equality Act;
- (2) the Swiss Disability Discrimination Act 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 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, information and activities will be classified, their value estimated, and behaviour 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, the 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 (inadvertently) discriminate against employees. However, certain legal authors argue that the currently applicable legislation that 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 “National Cyber Security Strategy” or “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 (NCSC), which, among other tasks, serves as a contact point for market actors. The Swiss Federal Council approved the new NCS on 5 April 2023, which outlines the objectives and measures through which the federal government, cantons, business community, and universities aim to combat cyber threats. Since 1 January 2024, the NCSC has become a Federal Office, designated in German as the “*Bundesamt für Cybersicherheit*”.

There is currently no overarching cybersecurity act nor any political agenda for the adoption of such regulation. However, the new Information Security Act, which is aimed at federal authorities and entered into force on 1 January 2024, has been revised to include as of 1 April 2025 a reporting obligation for operators of critical infrastructures. The NCSC acts as the central reporting office for cyber-attacks. The reporting obligation under the Information Security Act applies to operators of critical infrastructures, such as, among others, energy providers, financial services, healthcare providers, transportation, telecommunications, search engines and cloud services, etc. Cyber-attacks that have the potential to create significant damage must be reported.

Currently, Swiss data protection legislation often remains the starting point for any assessment of cybersecurity practices. The FADP, as well as the Data Protection Ordinance, call for state-of-the-art data security measures without specifying technical standards. The FADP thus maintains a future-proof and technologically neutral design. Additionally, the FADP contains a duty to report, in certain circumstances, data breaches to the competent data protection authority (the Federal Data Protection and Information Commissioner) or even the data subjects directly.

It is important to note that, under the FADP, individuals who intentionally fail 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 FADP, companies may also be criminally fined – up to CHF 50,000 – if an investigation on determining the responsible natural person within the company or organisation would entail disproportionate efforts.

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.



## **Acknowledgments**

The authors would like to thank Hai Nhu Pam and Anne-Sophie Morand for their work on the previous editions' Switzerland chapters.

**Jürg Schneider**

Tel: +41 58 658 55 71 / Email: [juerg.schneider@walderwyss.com](mailto:juerg.schneider@walderwyss.com)

Jürg Schneider is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. His practice areas include information technology, data protection and AI. Jürg has deep and extensive experience in the fields of data protection, information security and AI, with a particular focus on transborder and international contexts. His competencies include leading and assisting compliance projects on the implementation of requirements applicable to AI for Swiss and international companies, in particular in regulated sectors (banking, insurance, healthcare, etc.).

**David Vasella**

Tel: +41 58 658 52 87 / Email: [david.vasella@walderwyss.com](mailto:david.vasella@walderwyss.com)

David Vasella is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. He advises Swiss and international companies and authorities on questions concerning data and technology law. David specialises in data use, data and technology-related contracts, data security matters, cloud projects, data protection compliance and AI. He regularly gives talks and writes publications, for example on [datenrecht.ch](http://datenrecht.ch), a Swiss platform on data law. He is a certified information privacy professional and manager (CIPP/E, CIPM), fellow of information privacy (FIP) and AI governance professional (AIGP).

**Yannick Caballero Cuevas**


Tel: +41 58 658 83 69 / Email: [yannick.caballero@walderwyss.com](mailto:yannick.caballero@walderwyss.com)

Yannick Caballero Cuevas is an associate in the regulated markets, competition, tech and IP team at Walder Wyss, working in both the Lausanne and Geneva offices. He advises clients on data protection law, IT contracts, and regulatory issues relating to technology, including AI.

**Walder Wyss Ltd.**

Seefeldstrasse 123, 8008 Zürich, Switzerland

Tel: +41 58 658 58 58 / URL: [www.walderwyss.com](http://www.walderwyss.com)



**Global Legal Insights – AI, Machine Learning & Big Data** provides analysis, insight and intelligence across 22 jurisdictions, covering:

- Trends
- Ownership/protection
- Antitrust/competition laws
- Board of directors/governance
- Regulations/government intervention
- Generative AI/foundation models
- AI in the workplace
- Implementation of AI/big data/machine learning into businesses
- Civil liability
- Criminal issues
- Discrimination and bias
- National security and military

[globallegalinsights.com](https://globallegalinsights.com)