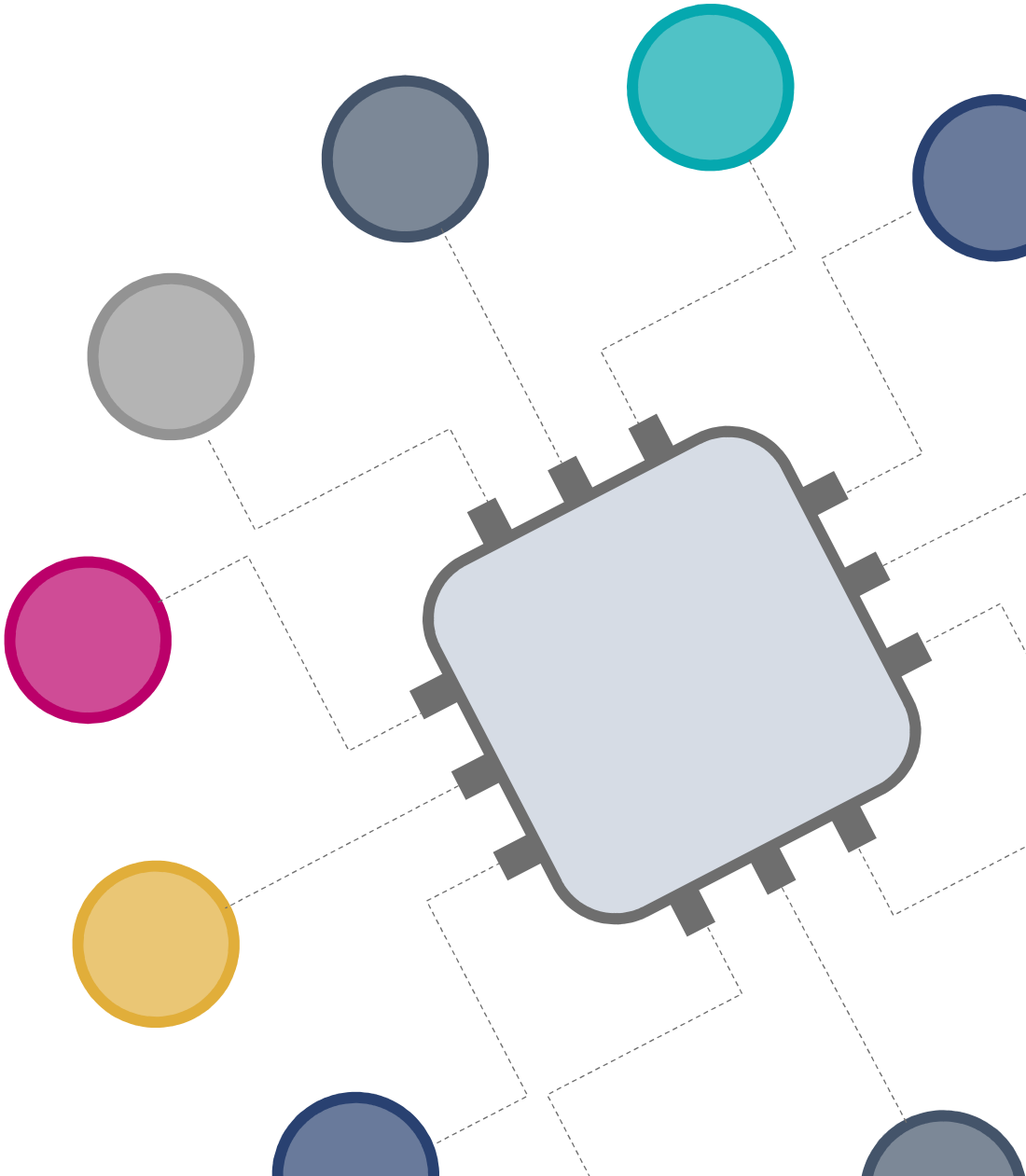
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Council

Bern, February 2022

Digital finance: areas of action 2022+



Contents

Executive summary

The ongoing digitalisation process is bringing about a sea change for the Swiss financial centre. Established location factors such as economic, financial and political stability, security and trust remain relevant. However, new elements such as the ability of companies and authorities to use new technologies are becoming more important for the future. On the financial market, new digital technologies are opening the door to new products and players, and challenging traditional financial service providers. How and by whom financial services are provided is fundamentally changing. In this report, this change process is referred to as "digital finance".

Given the speed and radical nature of the change, the Federal Council instructed the FDF to draw up a report on digital finance and to identify the Confederation's role and the specific areas of action. The report is intended to be the starting point for more in-depth work in the years ahead and to set corresponding priorities.

The financial market change process involves not only opportunities, but also risks for Switzerland as a business location. The continuously evolving digital technologies allow for the automation and flexible centralisation and decentralisation of processes, the elimination of third parties as intermediaries, and the recording of client behaviour and needs analysis for the most diverse and far-reaching purposes. Digital finance has great potential: efficiency, effectiveness and transparency can be increased, costs can be lowered, information asymmetries can be reduced and new partners and client groups can be attracted.

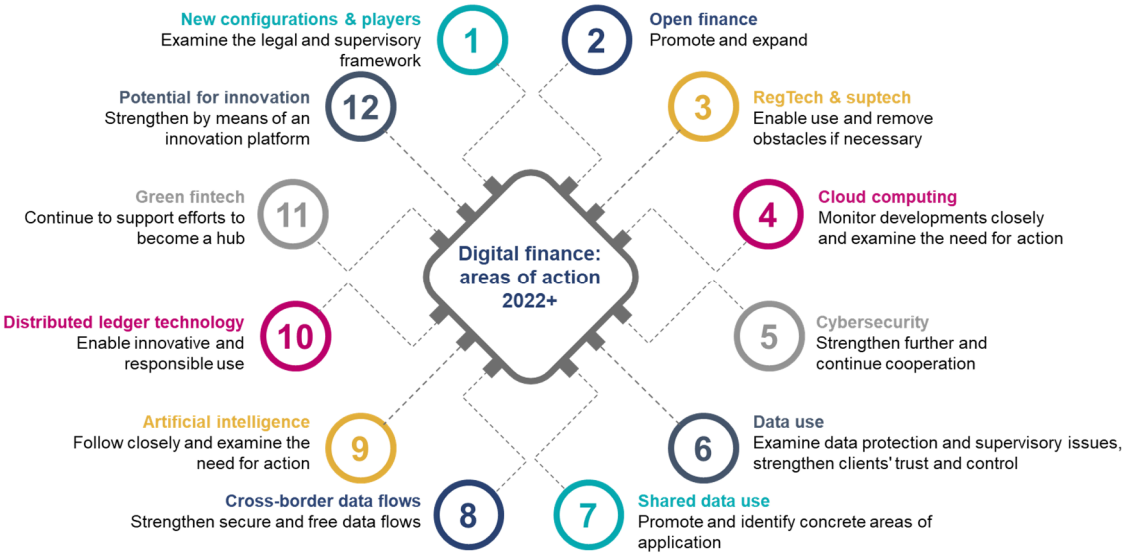
In terms of risk, the use of new technologies can increase vulnerability to cyberattacks, facilitate market manipulation or make it more difficult to combat money laundering and terrorist financing. The growing significance of data raises pressing questions about the protection of and control over personal information. Client protection remains a major challenge. With the dispersion of service provision among several players, the issue of responsibility and the competent contacts or complaints body arises in the event of problems, malfunctions or fraudulent acts. The fragmentation of value chains additionally increases the likelihood that a holistic view of possible operational risks does not exist and the dependence on third-party providers within the financial system rises.

The state has tasks to take on in the change process as well as in the new situation. The management and stabilisation of a status quo is being replaced by an all-round willingness to innovate while weighing up the risks. The innovation drivers of research and private sector entrepreneurship are responsible for the development and deployment of new digital technologies and products. The state's role is to provide the best possible framework conditions. Change processes are to be enabled, risks are to be addressed, stability, integrity and international competitiveness are to be maintained, and the sustainability and interconnectedness of the financial centre are to be promoted. The guiding principles are technology and competition neutrality, and there is thus the aspiration to treat the same business models and the same risks equally.

The authorities:

1. provide the best possible regulatory framework and are open to its ongoing review and needs-based adaptation;
2. are active dialogue partners for the various stakeholders (financial institutions, consumers, suppliers, innovative startups, operators of decentralised networks, globally active technology companies, academia) and coordinators in the case of market imperfections; and
3. work on cross-cutting issues with regard to competitiveness, financial stability risks, client protection and the reputation of the Swiss financial centre, specifically relating to the use of data, clouds, distributed ledger technology (DLT), cybersecurity, artificial intelligence (AI), green fintech, teaching and research.

The Federal Council is hereby setting out twelve areas of action with specific measures and instructing the FDF to implement these measures. The work is to be carried out in close coordination between politicians, authorities, the private sector and academia.



1 Quality of the financial centre location in a digital world

New location factors

The ongoing digitalisation process is bringing about a sea change for the Swiss financial centre. Established location factors such as economic, financial and political stability, security and trust remain relevant. However, new elements such as the ability of companies and authorities to use new technologies are becoming more important for the future.[1]

Digital finance

On the financial market, new digital technologies are opening the door to new products and players, and challenging traditional financial service providers. How and by whom financial services are provided is fundamentally changing. In this report, this change process is referred to as "digital finance".

Mandate and integration into financial market policy

Given the speed and radical nature of the changes, the Federal Council instructed the FDF to draw up a report on digital finance and to identify the Confederation's role and the specific areas of action (Federal Council objectives for 2021, volume II). That mandate is fulfilled with this report.

The report is intended to be the starting point for more in-depth work in the years ahead and to set corresponding priorities. The work is to be carried out in close coordination between politicians, authorities, the private sector and academia.

The report is part of the implementation of the Federal Council's financial market strategy of December 2020.[2] It is embedded in the Federal Council's objectives for the legislative period (guideline 1) and the Digital Switzerland strategy (core objective 4 – Ensure value creation, growth and prosperity).[3]

"Existing and new financial centre players must be able to make optimal use of the many opportunities offered by new technologies and data-driven business models. To enable this, the Federal Council is creating a technology-neutral regulatory framework for digital access, digitalising the interfaces with the authorities and promoting innovation in the financial sector."

Figure 1: 2020 financial market strategy

[1] This is confirmed by the methodology of renowned international rankings such as the IMD World Digital Competitiveness Ranking or the WEF Global Competitive Index, whose methodology was revised in 2018 due to digitalisation

[2] Federal Council report entitled "Leading worldwide, rooted in Switzerland: Policy for a future-proof Swiss financial centre" of 4 December 2020; source: www.sif.admin.ch > Documentation > Publications > Financial market policy > Report

[3] Digital Switzerland strategy of 11 September 2020; source: www.bk.admin.ch > Digital Transformation and ICT Steering > Digital Switzerland > Digital Switzerland strategy

1.1 Opportunities and risks for Switzerland as a business location

Key issues

Paying, saving, investing, financing and insuring are fundamental functions of the financial system, and will remain so. However, the use of new digital technologies on the financial market is opening the door to new products and players (see Figure 2: Digital finance overview).

The key issues are: How and by whom will functions currently fulfilled by money and financial services be performed in the future? Is there a need for action by the Confederation in this regard, and if so, what is it?

New technologies

The change process is based on the ongoing development of digital technologies, namely the continuous rise in storage capacity and computing power, digitalisation, increased networking via the internet, growing interaction between man and machine, the analysis of large volumes of data, the emergence of interconnected data centres (cloud computing), encryption techniques, distributed ledger technology (DLT) and mobile communication.

New products

These technologies enable, for instance: the automation of repetitive, manual, time-consuming or error-prone activities and processes; the provision of financial services at any location; the monitoring of client behaviour and the analysis of their needs for the most diverse and far-reaching purposes; the development of reliable and potentially more efficient ways of presenting and transferring assets, fulfilling obligations, enforcing contracts and managing risks; and the elimination of third parties as intermediaries.

In practice, clients benefit from new products such as aggregation and information platforms, customised services, payment services on mobile devices, platforms for transferring and trading digital currencies and assets, crowd lending/funding and pay-per-use insurance.

However, aside from these client-facing products, the use of new technologies also leads to a multitude of new applications in the internal processes of financial institutions, between service providers and at supervisory authorities. If these applications are related to regulatory compliance, they are referred to as RegTech (regulatory technology), while those related to supervision are referred to as suptech (supervisory technology).

New players

Startups in the financial sector that specialise in new technologies (fintechs) tend to focus on individual links in the value chain, in contrast to the traditional providers with their broad range of services. Their lower personnel and infrastructure costs and faster innovation cycles often enable fintechs to charge lower fees for their services.

The new players on the financial market also include big techs, i.e. the globally oriented, mostly US or Chinese technology companies that have been able to grow into powerful market platforms with web services (search engines, social networks, trading platforms, etc.). On the one hand, big techs provide cloud computing for Swiss financial service providers and fintechs. On the other hand, they are increasingly offering their own financial services, such as payment services. At present, these services are still based on traditional regulated financial service providers and financial market infrastructures (credit card networks and payment terminals). Due to their huge user base and the corresponding analysis of data and the economies of scale achieved, big techs are in an ideal position to offer their clients tailor-made financial services that take all of their needs into account. This means that they could potentially gain a significant market share quickly if they were to launch a new service in the financial sector.

Aside from fintechs and big techs, specialised outsourcing and infrastructure services are also being offered by companies, some of which are outside the industry. This is made possible by standardised application programming interfaces (APIs) and data formats, improved cybersecurity and more reliable and faster data links. This means that process steps can be separated to a greater extent and even smaller process steps can be outsourced.

Traditional financial service providers are likewise investing in digital technologies, especially in internal IT and innovation, although historical and in-house IT systems and dependencies are often challenging. However, they additionally make targeted use of the potential of fintechs by creating their own, investing in them or integrating them. Traditional financial service providers also partner with new players, be it in the area of cloud computing, outsourcing and infrastructure services, or fintech products. Conversely, traditional financial service providers have started to offer IT services (e.g. software packages) or financial services (e.g. account management) to other service providers, which in turn allows them to achieve economies of scale in development and licensing.

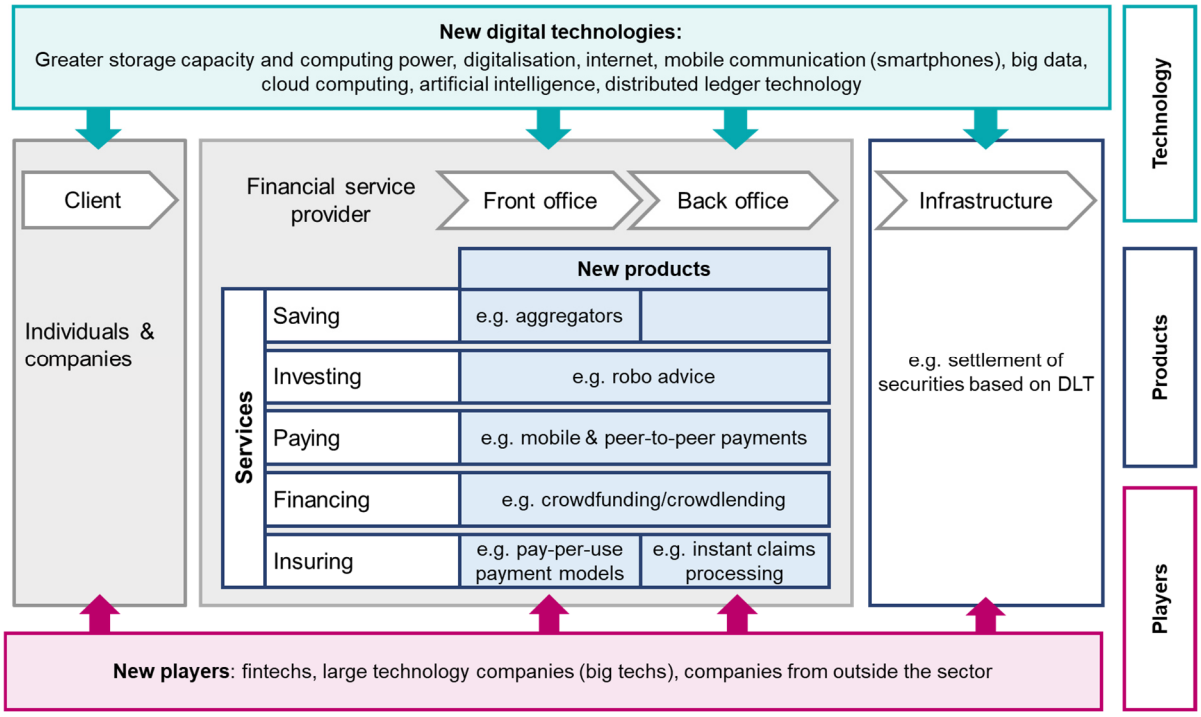


Figure 2: Digital finance overview

Significance of ecosystems

The use of new technologies and the establishment of technological standards (e.g. for APIs, data formats) significantly reduce the costs of coordination and interaction between the individual players, thereby promoting the creation of ecosystems that partly eliminate the boundaries between the financial sector and other economic sectors. Financial services can thus become an integral part of a larger ecosystem "outside the financial sector" (e.g. housing ecosystem with financial services such as mortgages or household insurance). In particular, this should enable a better purchasing and payment experience for clients.

Furthermore, a subdivision of services into modules and a fragmentation of the value chain can be observed in the financial sector, as it is no longer advantageous in some cases to develop all services internally.

Decentralised finance (DeFi) promises to create a completely independent value chain. DeFi describes an alternative financial ecosystem in which DLT-based financial services can be used in a decentralised manner and independently of financial institutions and the regulatory structures built around traditional banking. There are numerous possible applications for DeFi (e.g. trading platform, loans, insurance, stablecoins) and they have the potential to fundamentally change the financial sector.

For the Swiss financial centre, these developments are an opportunity to offer better services more efficiently by building on existing strengths. The modularisation of financial services and their dispersion among a larger number of players can potentially boost the system's overall resilience in the event of operational disruptions or cyberattacks.

However, modularisation can also increase vulnerability to cyberattacks, as there are more points of attack. The fragmentation of the value chain additionally increases the likelihood of not having an overview of potential operational risks, of becoming more dependent on third-party providers within the financial system, and of resulting in lower overall requirements for services than is the case today for comparable services (supplied by a single provider).

Furthermore, there is a risk of a diffusion of responsibility, leading to uncertainty both from a legal viewpoint (e.g. liability issues) and from a client perspective (e.g. lack of contact persons). The anonymity associated with digitalisation also heightens the risks of money laundering and the financing of criminal activities. These risks have to be taken into account in order to strengthen the Swiss financial centre and its reputation.

The authorities concerned therefore need to review the current regulatory and supervisory regime to see whether it needs to be modified. This also includes creating optimal framework conditions for innovation and cooperation in the financial sector. However, the authorities are also obliged to address the heightening of existing risks and the emergence of new ones, as well as to ensure that regulation and supervision in Switzerland continue to guarantee the stability and integrity of the financial markets and client protection.

Significance of data

The financial market is inherently data-driven and the use of data is an integral part of the core business of almost all financial centre players. The rise in digitalisation and networking has caused a manifold increase in the volume of data, the potential data sources and the analysis methods in recent years.

Dealing with data within a company and on the financial market has thus become a key issue even for financial market players (see box: SIF survey on data-driven business in finance). In this context, data within the company and its use between players is the basis, if not the essence, of the provision of most services in the financial sector, whereby the technological possibilities and the legal requirements set the framework (see Figure 3).

From a systemic perspective, improving the availability and quality of data can reduce information asymmetries and thereby increase transparency and effectiveness for financial system participants, regulators and supervisory

Box

Results of the SIF survey on data-driven business in finance: Swiss financial centre needs to catch up

SIF conducted a survey on data-driven business in finance among selected experts, associations and companies in the financial market sector in May 2021. The aim was to determine the current position of the Swiss financial centre concerning the economic use of data, measured against the technological possibilities, and to find out whether and how the framework conditions could be improved.

Around two thirds of the 32 participants believe that Switzerland is doing "a little less" or "a lot less" than other major international financial centres such as New York, London, Frankfurt or Singapore in terms of data-driven business. On the one hand, this is due to the fact that companies themselves are lagging behind, with organisational and cultural issues appearing to hamper the optimal use of data. Approximately 70% of respondents believe that companies do not make sufficient use of their internal data sources, and more than 50% also see considerable potential in other data sources, e.g. the use of data from companies outside the financial sector (64%), shared data use (data pooling, open finance) within the financial market (54%), the use of government data (54%) or the use of data from specialised providers (50%).

However, the survey participants are of the opinion that the greatest need for action concerns the authorities and the framework conditions they define. In their view, the authorities should act as a catalyst in the development of regulations, standards and standardised interfaces and platforms. Many respondents additionally believe that the supervision of data protection by the Federal Data Protection and Information Commissioner (FDPIC) should be clarified or simplified. Other areas for improvement include cybersecurity, while many survey participants and interviewees also see a need for action in the area of international agreements to improve legal certainty with regard to data flows, data protection and the possibility of access to data by foreign authorities. Another key theme concerns the confidentiality obligations under Article 47 of the Banking Act and Article 69 of the Financial Institutions Act, whereby these are mostly mentioned in the context of cloud outsourcing. The feedback on FINMA's supervisory practice is more varied, particularly in the case of concerns relating to outsourcing. Finally, more than 40% of respondents call for further improvements in access to government data.

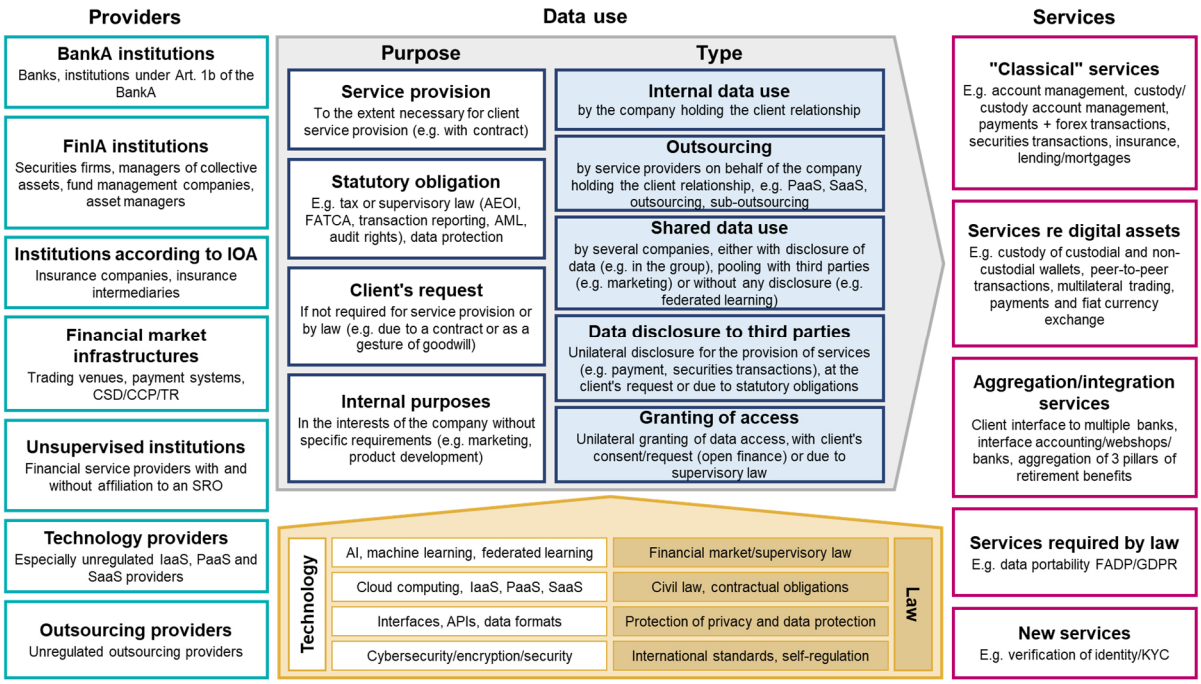


Figure 3: Use of data on the financial market

authorities alike in the fight against financial crime or when comparing sustainable financial services, for instance.

The growing significance of data increases the risks regarding the protection of privacy and control over personal information. A key challenge is that the new data applications can have complex implications for different areas of law. Aside from the aforementioned data protection, there are issues relating, for example, to the formation of oligopolies or even monopolies in the case of business models based on large amounts of data, and the barriers to innovation that these may present. Moreover, data is vulnerable to cyberattacks.

Automation (robotisation)

The automation of processes means that programmed or self-learning applications (AI) perform not only repetitive tasks, but also more and more tasks requiring a certain amount of thought and creativity which are new or were previously performed by humans. This likewise includes DLT-based autonomous protocols or programs (so-called smart contracts).

Automation can boost the efficiency of the financial system by either reducing the cost of providing services or improving their quality for the same cost.

However, automation can also lead to new risks from a financial market stability perspective, e.g. with regard to automated investment decisions, which can amplify price fluctuations and market volatility with similarly programmed decision-making criteria. In addition, automation requires that employees be retrained and leads to a greater need for skilled workers capable of developing, maintaining and managing the applications. Finally, it requires authorities, especially supervisory authorities, to acquire new skills.

Territorial decoupling and boundaries

Geographical distance has become much less relevant with the use of new technologies. Technologically speaking, a growing proportion of bank processes can be carried out entirely digitally. Local physical branches are not (or no longer) necessary for many lines of business.

This makes it possible to attract new partners or client groups, but it also increases cost pressure and the complexity of market positioning. This is especially true for geographically focused companies such as regional banks or regional branches of insurance companies.

At the international level, too, technological developments are opening up new opportunities for outsourcing or for recruiting skilled workers abroad. This poses a challenge for the state, which, unlike the industry, exercises its sovereignty only within its national borders, be it in the area of financial market supervision, financial crime deterrence and prosecution, data protection, cybersecurity, taxation or labour law.

In response to this, greater coordination can be observed at the international level, but also growing barriers to cross-border data flows. This includes the regulation of personal data protection (data protection, professional secrecy) and the properties or effects of software (regulation of platforms or AI). Another aspect concerns the increase in localisation requirements, which hamper international data flows. It is also worth mentioning the reinforcement of the regulatory safeguarding of national influence on critical infrastructures and the enforcement of stability and security requirements.

In some cases, these requirements hinder market access and are increasingly designed with extraterritorial effect. As a result, they lead to conflicts of law and legal uncertainty.[4]

Therefore, a location policy for digital finance must also take international developments into account and actively address them. In the process, the interplay between market access and financial market regulatory issues must be factored in, especially with regard to the regulation of new business models.

[4] "Foreign Economic Policy Report 2019, including dispatches on economic agreements and report on customs tariff measures in 2019", feature topic: digitalisation and foreign trade; 15 January 2020; source: www.seco.admin.ch > Services & publications > Foreign trade > Foreign economic policy > Foreign Economic Policy Report 2019

International competition regarding innovation

With the growing geographical decoupling, international competition regarding leadership in innovation and in certain areas is also intensifying. By international standards, Switzerland's current environment is favourable (a combination of high-quality globally active and well-established financial service providers, universities, legal certainty, research and development facilities, and infrastructure). For Switzerland as a business location, it is important to combine forces in Switzerland and work more closely together in order to boost the country's innovative power and make it visible to the outside world.

Interfaces with the authorities

The authorities are increasingly required to provide appropriate interfaces when cooperating with financial market players using new technologies. This includes the publication of legislative texts, access to government data, the keeping of land registers and commercial registers, and financial market supervision.

The provision of a state-recognised electronic means of identification (eID) is emphasised as a particularly important element by financial market players. Following the rejection of the Federal Act on Electronic Identification Services, the Federal Council instructed the Federal Department of Justice and Police (FDJP) to draw up a concept for a new eID solution. The public discussion on this and on possible technical solutions was completed at the end of the third quarter of 2021. Based on the results of this discussion, the Federal Council made a policy decision in December 2021. The draft of the new eID Act is expected to be put out for consultation in mid-2022.

In order to meet the new requirements, the authorities must provide digital services that enable financial market players to offer services (e.g. mortgage transactions or account opening) or processes (e.g. compliance with financial market law or RegTech) seamlessly, while being subject to the most efficient supervision possible.

1.2 The role of the Confederation

Tasks of the authorities

The state has tasks to take on in the change process as well as in the new situation. The management and stabilisation of a status quo is being replaced by an all-round willingness to innovate while weighing up the risks. The innovation drivers of research and private sector entrepreneurship are responsible for the development and deployment of new digital technologies and products. The state's role is to provide the best possible framework conditions. Change processes are to be enabled, risks are to be addressed, stability, integrity and international competitiveness are to be maintained, and the sustainability and interconnectedness of the financial centre are to be promoted. The guiding principles are technology and competition neutrality, and there is thus the aspiration to treat the same business models and the same risks equally.

The authorities:

1. provide the best possible regulatory framework and are open to its ongoing review and needs-based adaptation;
2. are active dialogue partners for the various stakeholders (financial institutions, consumers, suppliers, innovative startups, operators of decentralised networks, globally active technology companies, academia) and coordinators in the case of market imperfections; and
3. work on cross-cutting issues with regard to competitiveness, financial stability risks, client protection and the reputation of the Swiss financial centre, specifically relating to the use of data, clouds, distributed ledger technology (DLT), cybersecurity, artificial intelligence (AI), green fintech, teaching and research.

1.3 Status of the authorities' work

Confederation

Table 1 provides an overview of selected digitalisation projects already implemented or planned by the Confederation that are of relevance for the financial market. The Confederation has continuously checked the suitability of the existing framework conditions for the economic activities changed by new technologies and, weighing up the implications for all affected players, made specific adjustments to the legal framework where this was necessary to ensure legally secure use of technology that promotes innovation, as well as financial stability and client protection. Examples of this include the DLT bill, the reduction of formal requirements in financial market law and the creation of a fintech licence.

In addition, the Confederation has increasingly established itself as an active discussion partner for a growing number of players and as a national and international topic setter (e.g. FDF roundtables on open finance, digital banking, digital infrastructure and fintech, and active participation in conferences and panels). If necessary, it likewise stimulated the development of self-regulation, work on industry standards and the like in this way. An instrument that also supports the setting of topics in the area of digital finance abroad was created with the finance.swiss website, which bundles current information about the Swiss financial centre in one place and is aimed primarily at an international audience.

FINMA and the SNB

Aside from the Confederation's work, the Swiss Financial Market Supervisory Authority (FINMA) and the Swiss National Bank (SNB) are also active and have launched pioneering projects within the framework of their statutory mandates.

Notable examples at FINMA include the adjustments to due diligence requirements when entering into business relationships via digital channels (2016 and 2021), the establishment of a FinTech Desk (2016), the publication of clear guidelines for ICOs and the classification of tokens – the world's first regulatory authority to do so (2018), the granting of a banking licence to both financial service providers specialising in DLT (2019), the approval of a

financial market infrastructure that facilitates the trading of digital securities and their integrated settlement based on DLT (2021), the approval of a crypto fund (2021) and the specification of the expansion of resources in the area of cybersecurity and the corresponding reporting obligations (2021).

The SNB is involved in the Innovation Hub of the Bank for International Settlements (BIS) for innovation projects affecting central banking. For example, the Innovation Hub is developing a prototype new data architecture that will enable central banks to process market data from various trading venues in real time, thereby giving them a tool to monitor and analyse market conditions in fast-paced markets. In addition, the SNB, together with the BIS Innovation Hub, tested feasibility studies concerning the use of wholesale central bank digital currency (wCBDC) for the settlement of tokenised assets in central bank money for regulated financial institutions on a distributed ledger technology platform, as well as cross-border payments using wCBDC with the Banque de France.

To further improve the resilience of the financial system against cyber-risks, the SNB, together with SIX, launched the communication network Secure Swiss Finance Network (SSFN), which allows authorised participants operating in the Swiss financial centre to communicate more securely with each other and with financial market infrastructures.

	Implementation completed/in progress	Planned/being prepared
Fundamental elements for digitalisation	• Creation of the Digital Transformation and ICT Steering Sector (DTI), new steering mechanisms for the digital transformation of the authorities (2021)[5] • Data Protection Act reform (2020) and implementation (2021)[6] • Better protection against cyber-risks: National strategy for the protection of Switzerland against cyber-risks 2018-2022 (2019)[7] • More robust skills in ICT and ICT use (ERI dispatch – approved in Dec. 2020, action plan for digitalisation in the ERI sector in 2019 and 2020)[8]	• Legally recognised electronic identity (date to be decided) • Reduction of formal requirements & improved use of a qualified electronic signature (date to be decided) • Positioning of Switzerland as a location for data storage (from 2021)[9] • Strengthening of eGovernment: eGov & ICT strategy, cloud, national data management (NaDM), competence network for artificial intelligence (CNAI), Federal Act on the Use of Electronic Means for the Performance of Authority Tasks
Specific measures for digital finance	• DLT bill (2020-2021)[10] • Strengthening of cooperation on cybersecurity in the financial centre/crisis organisation in the banking sector (2020-2021)[11] • Further development of open finance (since 2020)[12] • Fintech licence (2019)[13] • RegTech/suptech report (2018)[14] • Regulatory sandbox (for banks 2017, for insurance companies 2021)[15]	• Measures based on this report

Table 1: Projects implemented or planned by the Confederation (selection)

[5] See: https://www.bk.admin.ch/bk/en/home/digitale-transformation-ikt-lenkung/bereichdti.html
[6] See: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html
[7] See: https://www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html
[8] See: https://www.sbfi.admin.ch/sbfi/en/home/eri-policy/eri-21-24/cross-cutting-themes/digitalisation-eri/Action%20plan%20for%20digitalisation%20in%20the%20ERI%20sector.html
[9] See: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-81573.html
[10] See: https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html
[11] See: https://www.efd.admin.ch/efd/de/home/digitalisierung/informationssicherung-in-der-elektronischen-kommunikation.html
[12] See: https://www.sif.admin.ch/sif/en/home/documentation/focus/open-finance.html
[13] See: https://www.finma.ch/en/authorisation/fintech/fintech-bewilligung/
[14] See: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-71341.html
[15] See: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73186.html

2 Areas of action 2022+

The Federal Council is hereby setting out twelve areas of action with specific measures and instructing the FDF to implement these measures. The work is to be carried out in close coordination between politicians, authorities, the private sector and academia.

2.1 New configurations and players

Fragmented service provision

Within the value chain in the financial sector, the distribution of services and products has already become fragmented. In addition to their own staff, providers often use third parties as external distribution partners (e.g. fund distributors or tied insurance intermediaries).

Similarly, "free" service providers (i.e. not affiliated to financial institutions) offer their support to clients at the point of sale (e.g. independent financial advisers or independent insurance intermediaries).

Configurations involving numerous players with a dispersion of services can be found in asset management (e.g. independent pension fund managers and asset managers) and in the infrastructure sector (trading systems, central counterparties, central securities depositories, payment systems), for example.

Dispersed service provision

In addition, clients are increasingly taking matters into their own hands and deciding for themselves how much dispersion they want. This development has been given impetus by the growing availability of data flow and exchange possibilities, namely open finance (see area of action 2.2).

Dispersed and collaborative service provision generates added value for both clients and providers. It allows clients to benefit from a broader choice of customised, innovative and sustainable solutions, while providers can focus on their core business, thereby eliminating development risks and costs, for example.

In a more fragmented value chain, it is important for providers to know to what extent they can rely on the steps taken by upstream or parallel providers as regards compliance with supervisory requirements and to what extent they can use the results of that work (identification of the contracting party, provision of information on investment risks, etc.), and what obligations they have with regard to selection, instruction and monitoring.

From a supervisory and client perspective, it is also important to know who is responsible for what and how individual risks are addressed (particularly operational resilience).[16] Decentralisation (especially of products based on DLT and smart contracts) and technology-driven fragmentation of the value chain mean that supervisory responsibilities are becoming increasingly difficult to assign and service providers sometimes move outside the statutory supervisory perimeter.

Existing legal concepts for mandating or involving third parties may not be able to adequately cover configurations with dispersed and collaborative service provision, decentralisation, cloud solutions and the like, or may do so only to a limited extent.

Old licence categories and new players

New, specialised players (including from abroad) may bring innovatively implemented services requiring authorisation to the financial market. Moreover, it is also possible that companies that provide services outside the financial sector may fall within the scope of financial market law if they offer innovative ancillary services, either by providing additional services through financial intermediaries or by accepting deposits from the public. The existing array of licence categories partly lags behind market developments. Depending on the circumstances, the requirements of a licence category may prove to be so high that the additional activity is abandoned. However, there may also be configurations where no relevant licence category exists at all

[16] For a global (including cross-border) picture, see: Financial Stability Board (FSB), "FSB Report on Market Fragmentation", 4 June 2019, 4 ff.; International Organization of Securities Commissions (IOSCO), "Market Fragmentation & Cross-border Regulation", June 2019, 6 ff.; OECD Task Force on Financial Consumer Protection, "Effective Approaches for Financial Consumer Protection in the Digital Age", 4 October 2019, 5 ff.

(aside from requirements under anti-money laundering legislation, where applicable), resulting in the coexistence of regulated and unregulated players. If an in-depth review shows that an adjustment of the supervisory perimeter is warranted, new modular licence categories could be created[17], existing categories could be split[18], or existing categories could be retained but subdivided[19], in order to ensure appropriate integration and differentiation. A system of self-regulation or private certification is conceivable to supplement the licensing requirements under supervisory law.

Risk orientation as a guiding principle

In financial market law, the principle of risk orientation generally applies, meaning that activities that are comparable in terms of risk should be subject to similar rules (same business, same risks, same rules), not least in order to create a level playing field. Given the growing number of players offering independent and sometimes novel services and activities, a review of the existing legal and supervisory framework is warranted with regard to activities and risks. In this context, there may be configurations where comparable activities entail different risks (e.g. depending on the size and internal risk management of an institution). Conversely, it is also conceivable that different activities may have comparable risks (e.g. the debate on non-banks[20], previously referred to as shadow banks, as well as big techs). Particular challenges arise when clients become players themselves, e.g. in the case of complete dispersion or decentralisation, when they become part of a swarm or the like.

Measure

1 Examine the legal and supervisory framework with regard to new configurations and players

The Federal Council instructs the FDF/SIF, in cooperation with FINMA and with the involvement of the industry, to review the existing legal and supervisory framework with regard to the framework conditions for new players and forms of service.

In particular, the legal and supervisory frameworks (e.g. in terms of outsourcing, involvement of third parties, service provider chains, etc.) are to be reviewed with regard to the fragmentation of the value chain to see how they open up new possibilities for the dispersion of service provision, regulate responsibilities and risks and avoid duplication.

It is also necessary to examine whether, in view of the emergence of new players, the existing supervisory perimeter should be extended or whether alternatives such as self-regulation and private certification should be supported or declared binding. Furthermore, clarification is needed as to whether existing licence categories and requirements for ancillary activities need to be more differentiated.[21]

[17] Example: new licence categories for portfolio managers and trustees, embedded in a licence chain (Art. 2 and 6 of the Financial Institutions Act, in force since 2020)

[18] Example: splitting of the original banking licence into a banking licence in the narrower sense and a new fintech licence (Arts. 1*a* and 1*b* of the Banking Act, in force since 2019); pursuant to Article 52a of the Banking Act, the Federal Council will review the changes and report to Parliament in the course of 2022

[19] Example: simplifications for highly liquid and well-capitalised banks in categories 4 and 5 (Art. 47*a* et seq. of the Capital Adequacy Ordinance, in force since 2020)

[20] The FSB, which coordinates the global development and implementation of financial market standards, broadly defines the shadow banking system as "credit intermediation involving entities and activities (wholly or partly) outside the regulated banking system" (FSB report, "Shadow Banking: Strengthening Oversight and Regulation", October 2011)

[21] Similar recommendations were made by EU experts: Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), "30 recommendations on regulation, innovation and finance", Final Report to the European Commission, December 2019, 67 ff. and 82 f. (recommendations 13 and 24)

2.2 Open finance

Benefits for clients

Open finance refers to the practice of exchanging financial data over standardised and secure interfaces at the request of clients.

It encourages interaction not only among financial service providers, but also between financial service providers and third parties (e.g. technology companies). It thus promotes the creation of ecosystems and forms the basis for innovative new services. It enables clients to obtain an overview of all of their financial assets (bank accounts, securities, pension fund and other retirement assets, etc.) at the click of a button, to have the ecological footprint of investments calculated by third-party companies, to open a bank account more easily, to withdraw money with their smartphone at a shop checkout counter, to detect gaps in their occupational pension cover and to have their creditworthiness calculated quickly.

This paradigm shift aims to give clients some control over their data and to put them at the centre of corporate strategy. This is the clearest manifestation to date of client self-determination in digital matters in the financial sector.

Innovation drivers

Standardised interfaces are a significant innovation driver that benefits both traditional financial institutions and fintechs. Among other things, established financial institutions can offer their clients a wide range of bespoke solutions without ceasing to focus on their core areas of expertise. In return, fintechs gain access to existing client relationships, if clients so wish.

While standardised interfaces are still in their infancy in the financial sector, their potential is already being increasingly exploited by comprehensive software-as-a-service solutions. The consistent implementation of open finance offers the Swiss financial centre an opportunity to significantly strengthen its innovative power. It is crucial that not only payment transactions, but also securities transactions or pension fund assets, among other things, are included and that fintechs are given structured, unbureaucratic access to the data of clients who so wish.

The Swiss approach

Unlike other countries, Switzerland is refraining from obliging regulated financial institutions to use open interfaces for the time being. Instead, the Federal Council expects the private sector, together with interested stakeholders, to push ahead with the standardisation and opening of interfaces in the various areas. This approach, which may be a little slow at first, could pay off in the longer term by concentrating investments in the most promising areas. For example, Switzerland is already playing a pioneering role in some open finance areas (e.g. custodian bank data).

However, this approach requires the active participation of traditional financial institutions. Therefore, the opening of interfaces must be explicitly encouraged by the Swiss authorities, in close cooperation with the industry. A more mandatory approach must remain an option in case developments in the market prove to be too slow or do not go far enough, thereby preventing the creation of new, innovative offerings and the potential for efficiency.

In December 2020, the Head of the FDF chaired a roundtable discussion with leading industry players on concrete approaches to promote open finance. SIF organises a quarterly strategy forum with key stakeholders to informally discuss the strategic direction and the need for action.

This includes an analysis of the possibilities or requirements for unregulated institutions to gain access to client data of regulated institutions. Standardisation of access, in a form and manner to be defined (e.g. private sector certification or a new type of financial market authorisation), could facilitate due diligence procedures in the cooperation between regulated and unregulated institutions. This could reduce the time and costs involved in establishing and maintaining such cooperation. Liability issues are also part of these considerations.

Measure

2 Promote and expand open finance

The Federal Council instructs the FDF/SIF to continue to regularly review the need for action to promote and expand open finance.

The measures can include close cooperation with the industry, consideration of new content or regulatory proposals for the Federal Council. A holistic approach should be taken and ecosystem thinking pursued. Such an approach also means, for instance, that access to financial data is not limited to financial institutions, i.e. that players from other sectors of the economy can likewise gain access under certain conditions, and that the financial sector can benefit from the opening of interfaces in other sectors.

If the progress is deemed insufficient, e.g. with regard to client and investor interests, the Federal Council shall instruct the FDF/SIF to submit a proposal to it on possible measures, including the examination of a statutory obligation to open up access to data via standardised interfaces.

2.3 RegTech and suptech

Fintech for regulation and supervision

The provision of financial services and the offering of appropriate products are subject to regulatory requirements, whose implementation and observance are checked and supervised. The Federal Council prepared an overview of the use of innovative technologies in financial market regulation supervision in June 2018[22] and highlighted the importance of regulatory and supervisory technologies in its financial market strategy of December 2020[23].

Fedlex, the completely updated, publicly accessible online publication platform for federal legislation, has been in operation since the beginning of 2021. This platform is used to publish, in particular, the Federal Gazette (BBl), the Official Compilation of Federal Legislation (AS), the Classified Compilation of Federal Legislation (SR), i.e. the consolidated version of federal and international legislation, and the compilation of international treaties applicable to Switzerland.[24] This comprehensive publication platform provides private individuals and companies with secure online access to all federal legislation (incl. directives and ordinances from the Federal Council, FINMA and the SNB). Tertiary legislation, such as FINMA circulars or recognised self-regulation rules, cannot be accessed via the publication platform at present.[25] In order for private individuals and companies to have seamless access to the legal rules and implementing provisions that are relevant and applicable to them, efforts should be undertaken to ensure further integration of data models and the relevant standards.

Machine-readable law

The requirement adopted by Parliament, whereby publications on the platform will generally have to be machine-readable, will enter into force in 2022[26]. This requirement will be implemented by publishing the texts of the AS, SR and BBl in XML (Extensible Markup Language) format in addition to PDF format. The Federal Chancellery is thereby using internationally recognised standards with which legislative, judicial and executive documents can be displayed in a structured way.[27]

With this standard, a first key prerequisite for RegTech applications has been created: legal texts are available in a structured format up to the level of individual paragraphs. For example, this allows a comparison of legislative provisions across different language versions, or automatic identification of changes at the level of individual articles or paragraphs.

[22] Federal Council report of 27 June 2018 on the use of innovative technologies in financial market supervision and regulation; source: www.efd.admin.ch > The FDF > Legislation > Reports > Other reports

[23] Federal Council report entitled "Leading worldwide, rooted in Switzerland: Policy for a future-proof Swiss financial centre" of 4 December 2020; source: www.sif.admin.ch > Documentation > Publications > Financial market policy > Report

[24] See: www.fedlex.admin.ch

[25] Standards of international organisations and bodies, and internal regulations of financial service providers are in any case not included, as they do not count as "federal legislation"

[26] See Article 1*a* paragraph 2 of the Publication Act

[27] Especially the European Legislation Identifier (ELI) standard; https://eur-lex.europa.eu/eli-register/about.html

Another important goal of the Federal Chancellery's current project work is to allow the data on the federal law platform to be used as part of the "semantic network" in line with the principles of linked open data.[28] This means that computers not only understand inputs, but can also put them into context against other meanings. For instance, the term "bank" can refer to both the river's edge and a financial institution. Whereas humans can infer what is meant on the basis of the context, machines first have to be taught to do this. For this purpose, individual legal provisions can be linked with additional information, i.e. metadata. An example of such metadata is the date on which a norm enters into force: while the legally binding version is the one in the legislative text in prose form, the version that has the most practical relevance for both humans and machines and is most often used for searches or analyses is likely to be the date of entry into force provided in structured form in the metadata of the federal law platform. An additional, more complex and currently unimplemented example could be the tagging of all articles containing reporting requirements.[29]

A beta version of the knowledge graph of the federal law platform is accessible in open data format for search queries, and can be freely used for analysis or to create new public or private services.[30]

Efficiency and effectiveness gains

Applications for RegTech range from the opening of client relationships, the monitoring of risk (credit, market, liquidity and operational risk), trading and portfolio management to reporting and disclosure requirements.[31] In this way, applications can learn how to identify and assess risks in the future, for example. Computers can also be trained to acquire a natural understanding of language (written, spoken, signed) and to use it to communicate. Whereas the demand side ultimately constitutes the supervised persons and entities, the supply side contains not only well-established technology companies, but increasingly also young startups. In a few cases, supervised persons and entities even occupy this business segment vis-à-vis third parties.[32]

Risks

As well as the sought-after efficiency and effectiveness gains, there are also risks associated with RegTech solutions. The high degree to which individual applications are data-driven requires high data quality, availability and reliability (e.g. the algorithms used). Additional risk concentrations in procurement, security risks and possibly even systemic risks are conceivable. As mentioned, only some of the companies on the supply side are subject to supervision. If new technological solutions are used or new technology-based business models are chosen, the manner in which the institution concerned deals with the associated risks is decisive. This concerns, among other things, the IT architecture, data management, the outsourcing framework, security, including cybersecurity and, where applicable, third-party risk management.

Supervision/suptech

As part of their activities, FINMA and the SNB, which are entrusted with supervisory and oversight tasks, also use suptech in addition to other supervisory instruments.[33] In this way, the implementation of and compliance with regulatory requirements (especially authorisation criteria) are checked and the risk exposure of an institution or the financial system can be

[28] Definition according to the World Wide Web Consortium (W3C); www.w3.org

[29] A prerequisite for this work is the creation and implementation of corresponding standards. One promising RegTech standard is LegalRuleML, issued by the OASIS standard-setting organisation in August 2021. This specification is in the form of an XML schema and aims to make the specificities of legal norms machine-readable in a broad, articulated and logical way: https://docs.oasis-open.org/legalruleml/legalruleml-core-spec/v1.0/os/legalruleml-core-spec-v1.0-os.html.

[30] See: https://fedlex.data.admin.ch/sparql; for a list of all concepts in the knowledge graph, see the predefined search "list of all triple store resources"

[31] The Institute of International Finance (IIF) defines RegTech as "the use of new technologies to solve regulatory and compliance requirements more effectively and efficiently" (IIF, "RegTech in Financial Services: Technology Solutions for Compliance and Reporting", March 2016, 3). For an overview, including on the technology used and statistics, see: Cambridge Centre for Alternative Finance, "The Global RegTech Industry Benchmark Report", 30 June 2019, 7 et seq.

[32] For an overview of the drivers, see: FSB, "The use of supervisory and regulatory technology by authorities and regulated institutions", 9 October 2020, 4 et seq.

[33] In a Financial Stability Institute (FSI) working paper, suptech is defined as "the use of innovative technology by financial authorities to support their work" (di Castri Simone, Hohl Stefan, Kulenkampff Arend and Prenio Jermy, "The suptech generations", FSI Insights on policy implementation No 19, October 2019, 4; this builds on Broeders Dirk and Prenio Jermy, "Innovative technology in financial supervision (suptech) – the experience of early users", FSI Insights on policy implementation No 9, July 2018, 3).

assessed, for example.[34] Moreover, FINMA's digital platforms (survey and application platform EHP, Trust Room and submission/delivery platform), which have been continually expanded over the last few years, allow authorisation applications and other enquiries to be submitted electronically. Specifically, data can be exchanged easily and without long time lags (or even in real time), although seamless usage has not been implemented for everything.[35] However, the physical channel remains relevant as, to date, there is no general obligation to communicate exclusively via digital channels.

Data innovation lab for supervision

To develop data-driven supervision further, FINMA is currently upgrading the technical prerequisites in order to collect quantitative data more easily. The aim for the future is to use more applications for intelligent and automated validation and plausibilisation of information. In order to go further and implement new applications for data-driven supervision, FINMA has set up a data innovation lab, where practical pilot projects are developed and, on the basis of an ongoing exchange between data scientists and supervisors, put directly into supervisory practice. The possible drawbacks could include a certain lack of transparency (e.g. clarity on how a specific decision was reached during an automated data evaluation solution). Moreover, the data sets could provide an additional incentive for cyberattacks.

Measures

3 Enable the use of RegTech and suptech

(1) The Federal Council instructs the FDF/SIF, in cooperation with FINMA and with the involvement of the industry, to identify possible obstacles to RegTech solutions and to examine the need for adjustments.

In the process, it should be examined whether and, if so, how it can be ensured that RegTech solutions which are planned or being developed can enable compliance with requirements in practice.

The Federal Council also expects those involved in the drafting of financial market legislation (administrations and affected parties) to consider at an early stage the extent to which aspects of a proposal can be implemented digitally. In this context, the obstacles to automated implementation (e.g. different definitions of terms, principles-based regulation) should be highlighted.

(2) The Federal Council welcomes the ongoing development of data-based supervision by FINMA and the integration of technological developments and suptech solutions into its activities.

The FDF/SIF shall also examine with FINMA and the Federal Chancellery the linking of FINMA regulations with the federal law platform.

[34] For instance, FINMA, on the basis of quantitative and qualitative data and an extensive system of indicators, automatically calculates the risk profile of supervised banks in the form of ratings. In addition, in the event of supervisory rules being infringed and relevant thresholds being breached, a fully automated alert is sent to the responsible supervisor once the corresponding data is available (so-called red flag alerts). For example, the SNB has created an online reporting system, eSurvey, which reporting institutions can use to transmit statistical data to the SNB electronically.

[35] In this regard, see: Federal Council report of 27 June 2018 (footnote 22), 10 et seq. and 18 et seq. – unlike FINMA, the SNB does not issue authorisations but can set requirements, especially for systemically important financial market infrastructures

2.4 Cloud computing

Advantages of cloud computing

Cloud computing allows computer resources (storage, computing power, etc.) to be obtained on demand as a service – usually via the internet – independently of the device, and to be billed according to usage. The use of cloud computing has a number of advantages, depending on the business model. These include shorter innovation cycles, increased scalability of services and high-performance computer systems without fixed capital costs for the user. The procurement of cloud services is now an integral part of many financial institutions' ICT procurement strategies, and is reinforcing the already observable trend towards outsourcing ICT to specialist vendors. Just as in the rest of Europe, Switzerland's cloud market is currently dominated by US vendors, followed by other international and national vendors.

Legal and technical questions partly resolved

Since the start of the current trend towards cloud computing, a number of legal and technical questions have been raised, both by financial institutions – especially banks – and by vendors and supervisors.[36] The focus is on questions around technology (e.g. technological dependence in terms of risks, system stability and lock-in), but also questions on legal uncertainty in the use and/or practicability of data protection, confidentiality obligations and banking secrecy, the US CLOUD Act, outsourcing and data protection law. Various developments have taken place in this regard which have helped to clarify these questions, at least partly:

- FINMA has overhauled its supervisory activity in the area of outsourcing and has clarified certain aspects of practice together with the financial sector and service providers (including adjustments to the outsourcing circulars of 2019 and 2020). In addition, it engages in regular exchanges with the industry, including ICT vendors, on issues surrounding cloud outsourcing.
- The Swiss Bankers Association (SBA) has published guidelines[37] and two legal opinions on cloud computing, as well as an appendix on audit issues.
- Various vendors have begun to develop services and contracts specifically tailored to the financial sector, in order to respond to the industry's reservations and concerns, and take their legal and supervision-related concerns into account.
- On 30 June 2021, the FDFA submitted a report to Federal Council which illustrates how Swiss legislation is also applied and enforced with respect to "Swiss" data abroad while simultaneously ensuring the greatest possible freedom of data flows and data use. At present, concrete measures to clarify official access rights are being examined by the competent units. The FDFA (Directorate of International Law (DIL) is coordinating these efforts, and will report to the Federal Council at the end of 2022.

Concerns about possible infringements of confidentiality obligations have generally declined among market participants. This was achieved through the increased use of technical and organisational security measures in financial institutions' outsourcing of client data, among other things. Often, a waiver with regard to certain legal obligations was also obtained, in order to release the institutions and their employees from any consequences under criminal law that might arise from confidentiality obligations.

Cloud computing appears to have advantages in terms of protection from cyberattacks and physical threats too. The specialisation of cloud vendors and their considerable investment in security can result in greater protection from cyberattacks, for example.[38] Specialist cloud vendors often lead the pack as regards physical security and the opportunities for storing data in geographically separate data centres (whereby, for example, protection against natural disasters, power cuts or fire is enhanced). Increasingly, large

[36] In its report published at the end of 2019, the FSB provided a comprehensive discussion of the advantages and drawbacks of cloud computing from a stability perspective

[37] Swiss Banking: Cloud computing

[38] Gartner forecasts that by 2025, 99% of security lapses in the cloud will be attributable to the clients rather than the vendors; see https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

cloud vendors are also offering solutions that allow their clients to restrict the permanent storage of data (so-called data at rest) to data centres in predefined regions.

Need for greater clarity in supervisory practice

Nonetheless, significant challenges remain concerning the use of cloud computing by regulated financial institutions. FINMA's supervisory practice, although technology-neutral, continues to be named in the SIF survey on data-driven business in finance (see section 1.1) as the greatest challenge facing the authorities in cloud outsourcing. Specific criticism is levelled at the different requirements for insurers compared to other financial service providers; these stem mainly from different legal frameworks.[39] With cloud services in particular, the outsourcing circular's requirements for subcontractors, e.g. as regards audit and termination rights, often presents difficulties. In addition, more clarity on supervisory practice is demanded on various topics (e.g. outsourcing abroad, cloud outsourcing) and questions arising at the interface between financial market supervision and data protection oversight.

US CLOUD Act

There are also outstanding questions on the US CLOUD Act, especially with regard to the need for an agreement with the United States spelling out the circumstances under which the relevant prosecution authorities can invoke the US CLOUD Act to demand the surrender of data stored in the other country, and which procedural rights apply to the directly and indirectly affected companies and citizens of both countries. This question – and thus the general question of the legal options for accessing data in an international context – is being examined in depth as part of the work, led by the FDFA (DIL), on official access rights, including on the basis of a corresponding report from the Federal Office of Justice.[40]

Data protection: EU adequacy decision

In order to allow data flows to be as unrestricted as possible, the EU adequacy decision confirming the equivalence of Swiss data protection legislation is of particular relevance for Switzerland. In cloud services, different data protection systems result in legal uncertainty and increase the effort required to implement different standards. For further explanations, see area of action 2.7.

Systemic risks

In addition, a number of authorities are identifying new systemic risks, such as the danger of vendor lock-in[41] and an oligopoly in an increasingly important financial market infrastructure.[42] The concentration in a few dominant vendors (so-called hyperscalers) based in only a few countries (e.g. the US) can lead to significant dependencies and should be examined in more depth from a risk perspective.

Measure

4 Closely monitor developments in cloud computing

(1) The Federal Council instructs the FDF/SIF, in cooperation with other affected units and the industry, to monitor developments in cloud computing and to examine the need for action.

The dialogue with regulated financial institutions using or wanting to use cloud services and with cloud vendors should be expanded and the framework conditions should be reviewed, in particular with regard to legal certainty, efficiency, financial market stability (e.g. access to relevant data for supervisory purposes), data protection (e.g. unintentional access by third parties) and dependence on technologies and vendors.

(2) The Federal Council welcomes FINMA's forward-looking and market-oriented supervisory practice and the ongoing exchange about developments among the relevant players.

[39] Specifically: the authorisation requirement for major outsourcing insurance, where FINMA enforces a requirement for certain insurance data to be backed up in Switzerland. By contrast, at banks, which are likewise subject to the outsourcing circular, outsourcing does not in principle require authorisation.

[40] Downloadable at: https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html

[41] The lock-in effect is generally understood to be the reliance of clients on a product or technology. This reliance stems from the fact that changing is associated with higher costs and is thus not attractive. If the technology is controlled by a single vendor, the client is de facto bound to the vendor and the phenomenon of "vendor lock-in" occurs.

[42] See, for example, https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0054-z - citeasputing

2.5 Cybersecurity

Cyber-resilience

A high degree of cybersecurity is essential for the digital economy to function smoothly. Companies operating in the financial centre are particularly exposed to the risk of attack and protect themselves accordingly, not least because a successful cyberattack affecting sensitive client data or assets can potentially have huge repercussions for the company concerned. But high resilience to cyberattacks is also a factor in the success of the financial sector and the business location as a whole. Moreover, an appropriate level of cybersecurity is important for an ecosystem based on the division of labour, in which shared use involves even sensitive data (see work on open finance).

2018-2022 national strategy

The Federal Council has recognised the significance of cybersecurity for the economy. In approving the 2018-2022 national strategy for the protection of Switzerland against cyber-risks, it introduced various measures to strengthen cybersecurity. With the National Cybersecurity Centre (NCSC) in the FDF – based on the well-established Reporting and Analysis Centre for Information Assurance MELANI – it also created an organisational unit capable of implementing the measures.

National Contact Point

The NCSC operates a National Contact Point to which the public can report cyberincidents and send their queries. In 2020, the Contact Point received over 10,000 reports, while the number is estimated at roughly double that for 2021. The NCSC also publishes current threat warnings and prevention guidelines on its website. In addition, it is involved in the analysis of vulnerabilities and, since the end of September 2021, it has been the accredited Numbering Authority in Switzerland, responsible for assigning CVE (Common Vulnerability and Exposure) identification numbers.

Reporting obligation

The FDF will further strengthen cybersecurity. It is currently drafting a proposal to introduce a general reporting obligation for cyberattacks. This should be aligned with the financial market's existing reporting obligations to FINMA. However, it will allow the reporting obligation to be extended to cover other sectors, and to establish the NCSC as the central reporting office.

Cooperation with the financial market

The project for "Increasing cyber-resilience in the financial market", which the NCSC is currently implementing together with partner organisations from the financial market, is specifically designed for the financial market. It is aimed at creating a viable structure for all financial market players to cooperate on cybersecurity, establishing an organisation for efficient crisis management and promoting the exchange of information.

Measures

5 Continue the cooperation on cybersecurity

The Federal Council instructs the FDF (NCSC), together with the competent offices (SIF, FINMA, SNB) to continuously monitor the threat situation and the state of progress regarding cybersecurity in the financial centre, and to expand the mechanisms for combatting financial cybercrime.

2.6 Data use

Economic potential

Compared to the technical possibilities, business models for data-driven business in the financial market are likely to still be underdeveloped and in their infancy (see the analysis conducted in 2021 on behalf of the Federal Institute of Intellectual Property, and the SIF survey on data-driven business in finance [see box in section 1.1]).

In Switzerland, there is no comprehensive regulatory concept covering data. However, various aspects of data and its use are regulated by different acts and ordinances. The use of government data is also subject to official secrecy.

Data protection

Data protection aims to flesh out the rights of the individual to privacy. In Switzerland, this is enshrined in Article 13 of the Federal Constitution. The Swiss Data Protection Act (FADP) has been completely revised in order to adapt it to the changed technological and societal landscape, and to ensure its compatibility with European data protection law. Data protection can also apply beyond national borders. One example is the European General Data Protection Regulation (GDPR), which also applies to companies and persons in Switzerland that process the personal data of natural persons in the EU when providing services to them (see area of action 2.8). Accordingly, aligning the FADP with the GDPR is crucial in order for the EU to continue recognising Switzerland as a third country with an appropriate level of data protection, and for the cross-border transmission of data to be possible without additional barriers in the future.

Data protection was a dominant topic in the survey and expert interviews. Overall, the legal framework – and the FADP in particular – is considered to be fit for purpose and relatively business-friendly. On the one hand, appropriate data protection is regarded as an essential requirement for unfettered data flows with the EU; on the other hand, as a fundamental prerequisite for maintaining clients' trust, it is seen as an inherent component of a business relationship.

However, in addition to data protection issues in an international context (see area of action 2.8), it is considered that action on the part of the authorities is necessary in a number of areas. As regards different directives and information from the Federal Data Protection and Information Commissioner (FDPIC), various industry representatives voiced a need for more nuanced supervision of data protection. For example, the FDPIC should indicate more clearly how new business models can be reconciled with the legal requirements concerning data protection, rather than just pointing out the legal risks. In the SIF survey (see box, section 1.1), the respondents generally mentioned legal uncertainty and the need for clarification. One example is the anonymisation of personal data. Here, the question of which steps might be sufficient in specific cases should be clarified, in order that anonymised personal data ceases to be regarded as personal data and its processing no longer falls under the FADP.

Banking secrecy

Financial market legislation also contains numerous provisions concerning access to, and the availability and usability of, data in different scenarios. The following aspects are often mentioned: rules on protecting sensitive data, especially client data; guaranteeing appropriate management of operational risks in data processing and the outsourcing of such processing; and obligations to store insurance data locally (see, among other things, FINMA-Circ. 08/21 on operational risks of banks (currently being completely revised) or FINMA-Circ. 18/03 on outsourcing).

In this context, professional secrecy rules for banks and other financial institutions (Art. 47 of the Banking Act, BankA, and Art. 69 of the Financial Institutions Act, FinIA) also have a significant influence on policy regarding the retention and processing of data by the institutions concerned and, where applicable, their service providers. This legislation provides for severe criminal penalties over and above the provisions of the FADP for the deliberate or negligent disclosure of client data to third parties.

Within the established financial industry and the world of politics, this continues to be seen as a locational advantage for Switzerland. By contrast, in the area of data management, this obligation also turns out to be a drawback, because it places additional hurdles in the way of institutions with data-driven business models and innovative data processing techniques. As a result, innovation is hampered and/or compliance costs are increased.

This is compounded by the way in which confidentiality obligations have changed over time (e.g. in connection with the now well-established automatic exchange of information) and additional legal uncertainty has arisen, meaning that confidentiality obligations now only apply in principle. Especially when disclosing client data to foreign officials, the boundaries of banking or professional secrecy are unclear, in light of the territoriality principle in criminal law. Further legal uncertainty surrounds the required form when obtaining banking secrecy waivers; no binding rules exist in this respect. As regards banking and professional secrecy, there is no supervisory authority that could provide clarity, as neither the FDPIC nor FINMA is responsible for this area, and the prosecution authorities act only as criminal prosecutors and not as supervisory authorities.

In practice, financial institutions deal with this challenge differently. A declining number of them explicitly use the confidentiality obligations under the BankA and the FinIA as an argument against outsourcing – at least in cases where client data could be accessed from abroad. Another group regards the confidentiality obligations as having been met – in line with the new SBA guidelines and the legal opinion prepared at the same time – if an institution takes appropriate technical and organisational measures (TOMs) when outsourcing or processing, and specifies them contractually. Lastly, there is a group that systematically uses the option to seek waivers from its clients with regard to confidentiality obligations, either completely or for specific scenarios.

In the Federal Council's view, a choice of options is welcome in principle. However, further analysis is needed to see whether the added value yielded by confidentiality obligations is justifiable in the long term. When financial institutions obtain blanket waivers from their clients, these obligations no longer have any effect. In practice, where these are aligned with data protection legislation without actually being identical to it, unnecessary legal uncertainty and implementation costs are created. In the short term, ways of increasing legal certainty about banking and professional secrecy should be examined.

Given the lack of uniformity in the current situation, we have not made any specific recommendations for action. The FDF/SIF will continue to monitor the use of confidentiality obligations against the backdrop of technological developments and with a view to reducing the possible costs of regulation. Going forward, bringing greater precision to banking secrecy, especially with regard to foreign aspects, should also be examined in more depth.

FINMA's supervisory practice

FINMA's supervisory practice is also regarded as a challenge in the context of economic data use (for FINMA's supervisory practice in the case of cloud outsourcing, see area of action 2.4). However, the specific concerns vary widely. They include overlapping protection requirements and responsibilities under the FADP and under the requirements on operational risks when handling critical and/or sensitive data at supervised entities (FINMA-Circ. 08/21 on operational risks, Annex 3 – currently being completely revised). There are also calls for intensified cooperation between the FDPIC and FINMA, in order to better clarify such boundary issues. It should also be noted that FINMA has no powers as regards banking and professional secrecy, or the application of the Data Protection Act. FINMA is tasked with monitoring the supervised entities' risk management and ensuring compliance with guarantee requirements, but not with defining the scope of professional secrecy and data protection.

Digital self-determination

In addition, the Federal Council has identified a need for further action in order to exploit Switzerland's data potential. At the same time, measures are needed to strengthen the public's trust in data use.

For this reason, the Federal Council instructed the DETEC and the FDFA to submit a report on fostering trustworthy data rooms while taking digital self-determination into account. The report will be published at the beginning of 2022 and will show how data rooms can be used to efficiently marry data supply and demand in a trustworthy manner. The digital self-determination approach is aimed at providing people with more control over their own data and with achieving more data use.

Measures

6 Support data use in the financial sector

The Federal Council instructs the FDF/SIF, together with the industry, the FDPIC and FINMA, to analyse the challenges of data protection practice and supervisory practice as regards data use in the financial sector, to assess the need for action and to foster cooperation between the players.

This is aimed at developing a nuanced understanding of the protection and use of data from the perspective of data protection and financial market legislation. There should also be a focus on how client trust and control in data use can be strengthened and wider data use can be fostered. In specific projects, unclear aspects should be tackled (e.g. concerning the anonymisation of personal data) and legal certainty in general should be reinforced.

Both the FDPIC and FINMA are to participate in these exchanges and provide the necessary resources, taking their statutory tasks into consideration.

2.7 Shared data use

Shared data use

In shared data use, participants' data is made accessible to the other participants under certain conditions, so that they can use it for their own purposes[43]. This can be done bilaterally or based on a shared or third-party operated platform.

Unlike the disclosure of data or the granting of access, the data use is not client or business case-specific. As a result, there is no request or consent from the client. Accordingly, transmission is limited to non-personal data, including anonymised and aggregated personal data. New technologies (e.g. confidential computing, federated learning) also promise the shared use of personal data (so-called collaborative analytics or data pooling), even without the data being disclosed.

The aim of shared data use is to improve knowledge-building from larger and more diverse data pools. In this way, algorithms can be better trained and calibrated on the basis of larger data pools. The insights gained can be used to better combat money laundering and terrorist financing, to mitigate cyber-risks or to optimise operations, products and distribution, for example.

At present, shared data use in the private sector is still largely theoretical. For a start, financial service providers such as banks and insurers still have little experience with shared data use and are therefore unable to assess its potential. Secondly, it is also not easy to coordinate the setting-up of such "common goods" between competing institutions. Thirdly, considerable legal uncertainty still surrounds shared data use.

Involvement of the authorities

Authorities can – and should – also participate in shared data use, especially as regards the provision of as much government data as possible, so long as there is a corresponding legal basis[44]. The Confederation already has a number of initiatives running on open government data, as well as the national data management project (NaDM). However, there is still a

[43] See report by the Swiss Federal Institute of Intellectual Property (IIP) on "Access to non-personal data in the private sector" of 1 March 2021

[44] In some circumstances, official secrecy can run counter to the expansion of such data use. For example, in principle FINMA can share only data that is in the public domain.

considerable need to catch up with the world's leading countries in this area. Moreover, there is a need to clarify how the initiatives mentioned above should be implemented by independent authorities such as the SNB and FINMA.

Share data use versus competitive advantage

Shared data use in the financial centre can be expected in areas where the participants value the knowledge gained from the larger and more diverse data pool more highly than the loss of the competitive advantage afforded by the exclusive use of data.

But shared data use also makes sense in areas where the financial centre as a whole benefits, such as fighting crime or promoting innovation. Here, clear governance and usage rules (incl. price setting) can create incentives for shared data use.

Governance and ICT standardisation

The implementation of shared data use requires efficient mechanisms for establishing common rules, governance (incl. regulating the responsibilities and risks) and the technical architecture (interfaces, standards, platforms) for data access/exchange and data use.

The European Commission's rolling plan for ICT standardisation[45] should inject new momentum into ICT standardisation, and the Swiss data economy should also benefit. SECO is leading current efforts to evaluate the options for expanding Swiss involvement in the relevant bodies at European and international level.

Data ownership rights

Another repeatedly mentioned challenge is the lack of property rights to data and databases in the Swiss legal framework. The Swiss Federal Institute of Intellectual Property's 2021 report examines this topic in detail. Despite the lack of specific property rights, current Swiss law contains many provisions that are similar to ownership: in particular, personal data is protected by data protection law, databases, as collections, can be subject to copyright in principle and, since 1 August 2021, rights of issue exist in bankruptcy with respect to data in general and cryptobased assets[46] in particular. In addition, the IIP has provided supplementary guidance[47] in the form of sample contracts aimed at simplifying contractual arrangements on access to non-personal data between companies. The Federal Council has already repeatedly discussed the need for specific data ownership under Swiss law and rejected the idea.

Initial efforts

The standardisation of interfaces and the prerequisites for access to data are key topics in the work on open finance, in which the FDF is involved (see area of action 2.2). The cooperation between the authorities and the various players in open finance could potentially serve as a model for fostering shared data use.

The creation of a central platform allowing access to data for new business models in the area of sustainable finance is being examined as part of the implementation of the green fintech action plan (see action plan, Action 1: "Foster access to data"[48]).

Switzerland is also involved in the Financial Action Task Force (FATF), in order to identify specific projects in which technology – in compliance with the relevant data protection provisions – has improved the exchange of information in private sector anti-money laundering and counter-terrorist financing efforts, and which can serve as examples for Switzerland.

Role of the private sector and the Confederation

In principle, creating the conditions for shared data use is a matter for the private sector, except for the necessary regulatory framework and the authorities' data and interfaces. However, the Federal Council has recognised the need for action in coordinating the players and clarifying legal aspects such as issues in anti-trust law, questions on the anonymisation of

[45] See: https://digital-strategy.ec.europa.eu/en/policies/rolling-plan-ict-standardisation

[46] See Article 4 of the Federal Copyright Act, Articles 242*a* and 242*b* of the Debt Enforcement and Bankruptcy Act

[47] See: https://www.ige.ch/en/intellectual-property/ip-and-society/data-processing-and-data-security

[48] See: https://www.sif.admin.ch/sif/en/home/documentation/focus/green-fintech-action-plan.html

personal data or on rights of use (data sovereignty or ownership) for data and client interests.

Measures

7 Foster shared data use in the financial centre

The Federal Council instructs the FDF/SIF, in collaboration with the financial sector and finance-affiliated ICT sector, as well as the affected units, to examine how shared data use in the financial centre can be promoted while taking account of the legal framework and client interests.

This includes the identification of concrete areas of application for shared data use, such as in combatting money laundering and terrorist financing.

For these applications, encouragement should be provided for bodies that create governance, usage rules and technical standards, interfaces or platforms for data access, data exchange and data use. The competent authorities are to support the participants in clarifying legal issues and creating legal certainty.

2.8 Cross-border data flows

Cross-border financial services

For the relatively small Swiss market, with the highly international focus of its financial institutions, a secure and cross-border flow of data complying with Swiss data protection and financial market requirements is very important. This includes the cross-border transfer, storage and processing of data. This applies both within a group (e.g. between the Swiss parent and subsidiaries or branches abroad, and vice versa) and between financial institutions located in Switzerland and service providers or clients based abroad (for cross-border data flows in cloud computing, see area of action 2.4).

The possibility of transferring, storing and processing data across borders is a decisive factor in market access. Accordingly, the conditions for data flows must always be taken into consideration in discussions on market access. The risks arising out of data storage abroad or in connection with access rights, conflicting norms or differing levels of data protection must likewise be taken into account.

Data protection in Switzerland

The FADP regulates the protection of personal data in data flows from Switzerland to other countries. If personal data is to be transmitted abroad, it must be ensured that this data is appropriately protected there. The FDPIC maintains a list of countries whose legislation guarantees appropriate data protection. However, data transmission to a country without appropriate data protection can be possible in some circumstances, for instance if appropriate protection in the destination country can be guaranteed contractually.

Data protection in the international context

By the same token, foreign jurisdictions appraise the level of data protection in Switzerland. Of particular relevance for intra-European data flows is the EU's recognition of Switzerland's equivalence, which is currently being examined. Moreover, in light of the ruling of the EU Court of Justice on Schrems II, the simplification rendered by the privacy shield in EU-US or Swiss-US relations lapsed without replacement. This has given rise to considerable new legal uncertainty surrounding the use of so-called standard contract clauses. This is a major problem for the entire Swiss digital economy, and the subject of discussions between the Federal Administration and its counterparts in the EU and US.

Foreign data protection law can also include an obligation to store and/or process personal data within national borders (so-called data localisation).

Swiss financial market law

The requirements under Swiss financial market law with regard to the transfer of data abroad and its storage and processing there refer to guaranteeing appropriate management of operational risks in data processing and the outsourcing of such processing, and the obligation to store insurance data

locally (see, among other things, FINMA-Circ. 08/21 on operational risks at banks or FINMA-Circ. 18/03 on outsourcing)[49].

Foreign financial market law

Abroad, the transfer of data to Switzerland and the processing of data in Switzerland are subject to the locally applicable requirements under financial market law. For some years now, a trend towards expanding the provisions on data localisation in financial market legislation has been observed. This involves requiring the storage and/or processing of certain data within national borders on regulatory or supervisory grounds. Likewise, access for auditors or FINMA to foreign service providers is sometimes challenging in terms of compatibility with the local law applicable to the service provider. This is especially the case when the service provider is self-regulating.

Currently, as regards intra-European data flows from a financial market law perspective, the European Commission's proposed Digital Operational Resilience Act (DORA) is significant. Its provisions on dealing with ICT risks also affect companies based in Switzerland that fall within the scope of DORA; these are generally companies that operate in an EU member state.

In addition, as regards criminal prosecution, the EU intends to set up a mechanism for prosecution authorities to access electronic evidence that is stored with internet service providers in another member state. It is planned to link this with a "domicile obligation" for internet service providers in the EU. This development should be monitored, also in terms of financial market law.

International efforts towards free data flows

At the international level, there are various efforts to ensure and foster cross-border data flows[50].

Since January 2019, a group of around 80 WTO members, including Switzerland, have been negotiating supplements to and clarifications of WTO rules on e-commerce. Important elements in these negotiations are possible provisions on ensuring free cross-border data flows, prohibiting the forced localisation of data storage and processing, and maintaining a legal framework to protect personal data (data protection). It is possible that additional sector-specific rules will be drawn up for the financial sector (incl. data localisation, e-payments, e-invoicing).

The prohibition of data localisation rules can also be found in free trade agreements, such as the United States-Mexico-Canada Agreement. Within EFTA, Switzerland itself has drawn up a finalised model text for future negotiations in EFTA.

Measures

8 Ensure free cross-border data flows

The Federal Council instructs the FDF/SIF to work with the other units and players concerned at international and national level to ensure free cross-border flows of financial data which comply with the requirements of Swiss data protection and financial market law.

This should include an examination of the impact of cross-border data flows on financial market access and financial stability, and a clarification of international aspects.

[49] For the significance of professional secrecy rules for banks and other financial institutions (Art. 47 of the BankA and Art. 69 of the FinIA) with respect to the handling of data, see area of action 2.6

[50] See also the section on focus areas in the Federal Council's 2019 report on foreign economic policy, especially section 1.2.5

2.9 Artificial intelligence

Disruptive potential

The growing use of artificial intelligence (AI) is among the remarkable and potentially promising developments in digitalisation. The use of AI applications such as machine learning, especially in combination with large amounts of data (big data), is seen as having disruptive potential. This is especially true for the data-intensive financial sector.

Issues concerning liability and use

The use of AI as an enabling technology can become a crucial success factor in the financial sector. Among other things, it allows for better personalisation of the services offered and also has great potential for risk reduction (e.g. when screening transactions).

However, the use of AI in the financial sector also raises important questions about the origin of data and its use, as well as the traceability of data processing, especially with regard to the traceability of decisions based on AI systems. According to the SBA, the main obstacle in the financial sector is the complexity of measures to ensure compliance with statutory requirements or ethical principles. Aside from client acceptance of AI and its technical implementation, legal and reputational risks are seen as the biggest challenges in the financial sector. Furthermore, AI systems may produce results (e.g. discrimination due to biased data) that raise social or even legal issues.

Shared data use

The issues in the area of AI are related to shared data use (see area of action 2.7). Firstly, this can lead to larger data pools, and these can in turn be used to better train and calibrate AI applications. Secondly, legal uncertainties surrounding AI (e.g. regarding responsibility for decisions made by AI applications) are impeding its more widespread use.

Overview

Against this backdrop, it is advisable to take stock of AI applications in the financial sector. The work started in a similar context in the field of blockchain/DLT could serve as a blueprint. Unlike in the area of DLT, the (national and international) visibility of the topic and the dynamics in the financial sector may not appear to be as high at first glance, as AI applications are usually not used directly for front-end processes, but rather in the back end. Nevertheless, like in the area of DLT, fundamental legal and ethical questions arise regarding responsibility for automated decision-making processes, for instance. The work of the interdepartmental Artificial Intelligence Working Group and, in particular, the artificial intelligence guidelines for the Federal Administration must be taken into account in this respect. At the international level, numerous processes are likewise dealing with these issues of AI regulation at present (e.g. in the Council of Europe or OECD). At the beginning of 2022, the FDFA (DIL) will submit a report to the Federal Council on the emerging international regulatory framework for AI.

Measure

9 Support the use of artificial intelligence in the financial sector

The Federal Council instructs the FDF/SIF, with the involvement of the other units concerned, to prepare an overview of the legal framework conditions in the area of AI applications that are of relevance for the financial sector.

The aim of the overview is, firstly, to provide a summary of the relevant legal framework conditions. Secondly, the open and proactive approach should highlight the potential for innovation and consistently reduce the risk of abuse and other risks. Thirdly, possible concrete needs for both legal/regulatory action and standardisation should be identified.

Furthermore, subject area leadership and active external communication on the use of artificial intelligence in the financial sector are to be established in order to promote innovation domestically and attract innovation activities from abroad.

2.10 Distributed ledger technology

Innovative Swiss regulation

Distributed ledger technology (DLT) enables consensus-based, distributed and synchronised registers to be held on a decentralised infrastructure (i.e. without a central administrator). The most common application of DLT at present is blockchain, which is characterised in particular by the use of cryptography. DLT and blockchain technology are among the most promising developments in digitalisation. In September 2020, Parliament adopted the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act). In a first step, the DLT Act made specific amendments to ten federal laws. Switzerland has thus created important framework conditions that are conducive to the use of these technologies in many areas and that will enable the country to establish itself as a leading and innovative location for fintech and DLT companies, and to further develop in that regard. At the same time, the DLT Act paves the way for combatting abuses more effectively and protecting the integrity and good reputation of the Swiss financial centre. The DLT Act and the associated blanket ordinance came into force in two steps in 2021.

Three pillars of the DLT Act

The DLT Act essentially comprises three pillars. First, the amendments to the Swiss Code of Obligations, the Intermediated Securities Act and the Federal Act on International Private Law allow for the introduction of ledger-based securities stored in a DLT-based register (usually on a blockchain). Second, the adaptation of insolvency law enables the segregation of cryptobased assets in the event of bankruptcy. Finally, the DLT trading facility has seen the creation of a new authorisation category in financial market law for DLT-based financial market infrastructures. The DLT trading facility enables multilateral trading of DLT securities according to non-discretionary rules. The entire DLT Act is generally technology-neutral.

Anti-money laundering

The DLT Act also closed potential gaps in the area of money laundering. DLT trading facilities and financial intermediaries that help transfer virtual currencies to a third party are now subject to the Anti-Money Laundering Act (AMLA). Similarly, issuers of virtual currencies which are actually used or intended by the organiser or issuer to be used as a means of payment for acquiring goods or services or as a means of money and value transfer are subject to the Anti-Money Laundering Act. The implementation of these legislative amendments is a challenge. The money laundering and terrorist financing risks associated with virtual currencies remain considerable and require effective coordination between the competent authorities and closer cooperation with financial intermediaries (see also area of action 2.7).

Coordination with the FATF and the OECD

Switzerland's amendments to the AMLA are in line with the work of the FATF on virtual assets. The FATF has updated its guidance for a risk-based approach to virtual assets and virtual asset service providers, and clarified various points. The guidance clarifies that the definitions of virtual assets and corresponding service providers are to be understood in a broad sense, and that the group of providers subject to the AMLA should thus be interpreted similarly broadly. Both the FDF and the FATF are actively following developments in this area.

The OECD is likewise taking account of DLT developments and is currently preparing a global standard for the international automatic exchange of information (AEOI) on virtual assets. The aim is to clarify the handling of virtual assets and their providers, and to create a level playing field with traditional assets and their providers, which are already subject to the AEOI. The new AEOI standard is expected to be adopted at the end of 2022. Switzerland is actively involved in this work. In due course, it will be necessary to examine whether the new AEOI standard should be incorporated into national law or whether the existing legal basis should be amended on an ad hoc basis.

Need for adaptation in the area of funds

In order to ensure that the benefits of DLT can be fully exploited in even more areas of law, it will be necessary in the future to examine which other federal laws need to be adapted.

At first glance, there appears to be untapped potential for the use of these new technologies in the area of the Collective Investment Schemes Act (CISA) in particular.

Funds can undoubtedly invest in digital assets already today, and FINMA recently approved the first cryptocurrency fund. Since the entry into force of the DLT Act, it has also been possible to issue fund units in the form of tokens. However, the CISA does not yet provide for the use of DLT for the custody and management of digital assets, which limits the potential for innovative new products and efficiency gains.

Consequently, the FDF, in cooperation with the industry and FINMA, should identify the obstacles that still prevent the efficiency benefits of these new technologies from being fully exploited, including in the area of collective investment schemes. If necessary, the FDF will then draw up a proposal to remove these obstacles (e.g. custodian bank requirements for investments in digital assets).

Measure

10 Enable innovative and responsible use of DLT in the financial sector

The Federal Council instructs the FDF/SIF, in cooperation with the industry, to strengthen the use of DLT in the financial sector and, in cooperation with FINMA, to continuously review the legal framework with a view to making regulatory adjustments.

In this context, subject area leadership and active external communication on DLT in the financial sector are to be expanded in order to promote innovation domestically and attract innovation activities from abroad.

As regards the Collective Investment Schemes Act, the FDF/SIF, in cooperation with FINMA and the industry, is to examine which hurdles still exist concerning the use of blockchain and distributed ledger technology and, if necessary, prepare a proposal to remove them.

2.11 Green fintech

Competitive advantage through excellence in asset management

Swiss banks manage around 27% of the cross-border assets under management worldwide. A generational shift is under way in this sector. Millennials are likely to increasingly invest their inherited assets sustainably and digitally. A financial centre that is at the forefront in both of these respects will therefore have a significant competitive advantage in asset management.

Moreover, the measures to combat climate change and the decline in biodiversity offer considerable opportunities for companies. Swiss green fintech solutions can help national and international companies take advantage of these opportunities and thereby boost their competitiveness.

Switzerland has recognised the potential of exploiting digital technologies in the area of sustainable finance and is positioning itself as a global leader in this field.[51] Accordingly, it is important to ensure that the right framework conditions are in place for Switzerland to become a hub for green fintechs. The term green fintechs refers to technology-based innovations that can be used for all kinds of financial processes and products and at the same time consciously support sustainability goals or reduce sustainability risks.

Green Fintech Network

In this context, SIF formalised a previously informal network of leading representatives of the green fintech sector. Within the framework of an action plan, the network developed possible ideas for companies wishing to increase their activities in the area of green fintech, as well as for further work by the Confederation.

[51] See the 4 December 2020 update of Switzerland's financial market policy

Two further core concerns of the green fintech sector were addressed by the Federal Council last year:

In summer 2021, the Federal Council adopted key parameters for future mandatory climate reporting by large Swiss companies in accordance with the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD). The Federal Council explicitly wants a standardised digital format for the disclosures, which is conducive to better access to sustainability data.

Furthermore, in autumn 2021, the Federal Council adopted measures to increase the transparency of financial products in order to combat greenwashing. Greenwashing occurs when clients are misled or deceived about the sustainable characteristics of financial products.

Transparency in financial reporting on climate issues

In the coming months, the Green Fintech Network will focus on work to improve access to sustainability data for Swiss green fintechs. Other objectives are to encourage the establishment of green fintechs in Switzerland, to simplify access to potential clients, and to increase the supply of risk capital in Switzerland.

In addition, Switzerland should actively position itself as a green fintech hub as part of its international commitment. For example, it is currently working on possible cooperation with Singapore to bring the Singapore FinTech Festival to Switzerland, with green finance being one of the thematic focus areas. This topic was also prominent the Building Bridges week in Geneva in November 2021.

Measure

11 Continue to support efforts to make Switzerland a leading green fintech hub

The Federal Council instructs the FDF/SIF to actively introduce green fintech as a topic in international bodies and sustainable finance initiatives, and to seek dialogue with the relevant national and international players.

In particular, transparency and the availability of data in this area should be promoted. Relevant bodies include the G20 Sustainable Finance Working Group and the International Platform on Sustainable Finance.

The FDF/SIF regularly informs the Federal Council about national and international work in the area of green fintech.

2.12 Potential for innovation

Middle of the range international ranking for Switzerland

Unlike the Swiss financial centre, which remains at the top of the global rankings, Switzerland is currently only in the middle of the pack as a fintech hub.[52] It has neither a significant number of so-called unicorns, i.e. fintechs valued at over USD 1 billion, nor can it regularly boast successful IPOs or company sales. Accordingly, Switzerland needs to build its international visibility and clout as a fintech hub. As a leading financial centre and location for innovation[53], this needs to be remedied.

No central platform

Although various players are already involved in teaching and research (e.g. Swiss Finance Institute), startup promotion (e.g. F10, Kickstart Innovation, InnoSuisse), contact points (e.g. FINMA's FinTech Desk), research and development, and knowledge sharing (e.g. BIS Innovation Hub), they have only a limited field of activity (sometimes due to the legal mandate of the corresponding institution, e.g. FINMA) or focus on specific sectors and are thus not in an ideal position to provide the advice required by fintech startups.

In particular, however, there is still no uniform platform for innovation and the exploitation of technology in the Swiss financial centre that could act as a one-stop shop to ensure the provision of information and coordination by the authorities. This hinders both the establishment of new fintech companies of foreign origin and coordination between existing market participants in Switzerland.

Need for interpretation regarding regulations and pioneering services

With the development and use of new business models that leave room for interpretation, startups and the innovation sector in general are in need of guidance. An independent body could help the industry to gain clarity in the development of innovative financial services.

Moreover, there are application scenarios and areas of activity where the development of common standards or overarching projects would generate added value for all financial market participants (e.g. data sharing, digital identity, certification of service providers or products). However, the costs and risks associated with this constitute a sort of first-mover barrier.

Networking across sectors

As described in section 1.1, the shift away from clearly delineated sectors towards overarching ecosystems and corresponding business concepts is becoming more pronounced. For example, financial services are increasingly being embedded in other processes in the real economy (embedded finance), e.g. when the payment for a transaction is only carried out automatically in the background. It seems sensible to provide for the possibility of greater exchange and cooperation here.

Bridge between empirical research and practice

Research and development lead to new technologies and innovation, and thus promote competitiveness, prosperity and employment. Switzerland is a leader in the area of basic research in the financial sector, as can be seen in the large number of articles published in renowned scientific journals.[54]

While the dialogue and exchange between researchers and practitioners is reflected in the range of continuing professional development courses[55], there is a lack of established and internationally recognised courses in tertiary education that enable research (in the area of technology and finance) and practice (application in financial market law) to be more closely interlinked.

Uniform innovation platform

In summary, aside from the classical role of legislator, the role of catalyst is gaining in importance in a digital financial centre, i.e. the presence of a uniform platform that relies on a collaborative approach with all stakeholders. Other countries and international organisations are also pursuing this approach in the form of labs, institutes or hubs.[56]

---

[52] This is reflected in major rankings such as the Global Startup Ecosystem Report 2021 and the Global Fintech Index City Rankings Report

[53] In the Global Innovation Index, for example, Switzerland has held the top spot every year since 2013; see https://www.globalinnovationindex.org/analysis-indicator

[54] In 2021 alone, more than 20 articles were published in major scientific journals; see https://www.sfi.ch/en/faculty/publications

[55] See, for example, https://industry.sfi.ch/en/sfi-master-classes

[56] See the FCA's Innovation Hub or LabCFTC, for example

Such a uniform platform, based on improved cooperation between established financial service providers, innovators, academia and regulatory and supervisory authorities, could make a valuable contribution, for instance in the form of an innovation lab, to better regulation (more closely aligned with the latest developments) and thus concretely promote innovation. Furthermore, it could help the industry to develop overarching projects, where the intervention of an authority as coordinator would be helpful.

Consultations with other competent authorities and with representatives from education and the private sector have thus led to the proposal to set up an innovation platform in the financial sector.

The objectives of such a platform could be as follows:

- Creation of a single point of contact with authorities for innovation in the financial centre (one-stop shop, hub of hubs)
- Removal of first-mover barriers through more extensive coordination and support of the industry in the context of overarching projects
- Reduction of legal uncertainty by means of practical guidelines and checklists for startups
- Exploitation of cross-sectoral synergies by creating exchange opportunities for players from different sectors
- Stronger networking of basic research and application in business, technology and innovation
- Positioning of Switzerland as a top fintech location through better coordination of the various players and based on the experience gained also on the part of the authorities

Measure

12 Strengthen the innovation potential of the financial sector in the long term by means of an innovation platform

The Federal Council instructs the FDF/SIF, in cooperation with the other bodies concerned and the industry, to submit a proposal to the Federal Council with specific objectives and a formal structure for an innovation platform for the financial sector.

Appendix: Overview of areas of action, measures and time frames

	Measures		*Time frames*
1 New configurations and players	Examine the legal and supervisory framework with regard to new configurations and players	The Federal Council instructs the FDF/SIF, in cooperation with FINMA and with the involvement of the industry, to review the existing legal and supervisory framework with regard to the framework conditions for new players and forms of service. *In particular, the legal and supervisory frameworks (e.g. in terms of outsourcing, involvement of third parties, service provider chains, etc.) are to be reviewed with regard to the fragmentation of the value chain to see how they open up new possibilities for the dispersion of service provision, regulate responsibilities and risks and avoid duplication.* *It is also necessary to examine whether, in view of the emergence of new players, the existing supervisory perimeter should be extended or whether alternatives such as self-regulation and private certification should be supported or declared binding. Furthermore, clarification is needed as to whether existing licence categories and requirements for ancillary activities need to be more differentiated.*	- Establishment of working group (2022) - Review and, if need be, initiation of adjustment of the legal and supervisory framework (by 2025)
2 Open finance	Promote and expand open finance	The Federal Council instructs the FDF/SIF to continue to regularly review the need for action to promote and expand open finance. *The measures can include close cooperation with the industry, consideration of new content or regulatory proposals for the Federal Council. A holistic approach should be taken and ecosystem thinking pursued. Such an approach also means, for instance, that access to financial data is not limited to financial institutions, i.e. that players from other sectors of the economy can likewise gain access under certain conditions, and that the financial sector can benefit from the opening of interfaces in other sectors.* *If the progress is deemed insufficient, e.g. with regard to client and investor interests, the Federal Council shall instruct the FDF/SIF to submit a proposal to it on possible measures, including the examination of a statutory obligation to open up access to data via standardised interfaces.*	- Active dialogue partner/coordinator and examination of the need for action (ongoing) - If necessary, proposal of measures for adjusting the framework conditions (by 2025)
3 RegTech and suptech	Enable the use of RegTech and suptech	(1) The Federal Council instructs the FDF/SIF, in cooperation with FINMA and with the involvement of the industry, to identify possible obstacles to RegTech solutions and to examine the need for adjustments. *In the process, it should be examined whether and, if so, how it can be ensured that RegTech solutions which are planned or being developed can enable compliance with requirements in practice.* *The Federal Council also expects those involved in the drafting of financial market legislation (administrations and affected parties) to consider at an early stage the extent to which aspects of a proposal can be implemented digitally. In this context, the obstacles to automated implementation (e.g. different definitions of terms, principles-based regulation) should be highlighted.* (2) The Federal Council welcomes the ongoing development of data-based supervision by FINMA and the integration of technological developments and suptech solutions into its activities. *The FDF/SIF shall also examine with FINMA and the Federal Chancellery the linking of FINMA regulations with the federal law platform.*	- Establishment of working group (2022) - Review and, if need be, initiation of adjustment of the legal and supervisory framework (by 2025) - Consideration of digital implementability when drafting financial market legislation (ongoing) - Active dialogue partner/coordinator for data-based supervision (ongoing)

4 Cloud computing	Closely monitor developments in cloud computing	(1) The Federal Council instructs the FDF/SIF, in cooperation with other affected units and the industry, to monitor developments in cloud computing and to examine the need for action. *The dialogue with regulated financial institutions using or wanting to use cloud services and with cloud vendors should be expanded and the framework conditions should be reviewed, in particular with regard to legal certainty, efficiency, financial market stability (e.g. access to relevant data for supervisory purposes), data protection (e.g. unintentional access by third parties) and dependence on technologies and vendors.* (2) The Federal Council welcomes FINMA's forward-looking and market-oriented supervisory practice and the ongoing exchange about developments among the relevant players.	- Active dialogue partner/coordinator and examination of the need for action (ongoing) - If necessary, examination of the legal and supervisory framework (by 2025)
5 Cyber-security	Continue the cooperation on cybersecurity	The Federal Council instructs the FDF (NCSC), together with the competent offices (SIF, FINMA, SNB) to continuously monitor the threat situation and the state of progress regarding cybersecurity in the financial centre, and to expand the mechanisms for combatting financial cybercrime.	- Active dialogue and examination of the need for action (ongoing)
6 Data use	Promote data use in the financial sector	The Federal Council instructs the FDF/SIF, together with the industry, the FDPIC and FINMA, to analyse the challenges of data protection practice and supervisory practice as regards data use in the financial sector, to assess the need for action and to foster cooperation between the players. *This is aimed at developing a nuanced understanding of the protection and use of data from the perspective of data protection and financial market legislation. There should also be a focus on how client trust and control in data use can be strengthened and wider data use can be fostered. In specific projects, unclear aspects should be tackled (e.g. concerning the anonymisation of personal data) and legal certainty in general should be reinforced.* *Both the FDPIC and FINMA are to participate in these exchanges and provide the necessary resources, taking their statutory tasks into consideration.*	- Active dialogue and examination of the need for action (ongoing) - Exploration of the topic for the financial market (ongoing)
7 Shared data use	Foster shared data use in the financial centre	The Federal Council instructs the FDF/SIF, in collaboration with the financial sector and finance-affiliated ICT sector, as well as the affected units, to examine how shared data use in the financial centre can be promoted while taking account of the legal framework and client interests. *This includes the identification of concrete areas of application for shared data use, such as in combatting money laundering and terrorist financing.* *For these applications, encouragement should be given to bodies that create governance, usage rules and technical standards, interfaces or platforms for data access, data exchange and data use. The competent authorities are to support the participants in clarifying legal issues and creating legal certainty.*	- Establishment of working group and examination of possible measures (2022) - Promotion of concrete areas of application (up to 2025)
8 Cross-border flow of data	Ensure free cross-border data flows	The Federal Council instructs the FDF/SIF to work with the other units and players concerned at international and national level to ensure free cross-border flows of financial data which comply with the requirements of Swiss data protection and financial market law. *This should include an examination of the impact of cross-border data flows on financial market access and financial stability, and a clarification of international aspects.*	- Active dialogue partner/coordinator (ongoing)

9 Artificial intelligence	Support the use of artificial intelligence in the financial sector	The Federal Council instructs the FDF/SIF, with the involvement of the other units concerned, to prepare an overview of the legal framework conditions in the area of AI applications that are of relevance for the financial sector. *The aim of the overview is, firstly, to provide a summary of the relevant legal framework conditions. Secondly, the open and proactive approach should highlight the potential for innovation and consistently reduce the risk of abuse and other risks. Thirdly, possible concrete needs for both legal/regulatory action and standardisation should be identified.* *Furthermore, subject area leadership and active external communication on the use of artificial intelligence in the financial sector are to be established in order to promote innovation domestically and attract innovation activities from abroad.*	- Preparation of overview (2022) - Active dialogue partner/coordinator and exploration of the topic for the financial market (ongoing)
10 Distributed ledger technology	Enable innovative and responsible use of DLT in the financial sector	The Federal Council instructs the FDF/SIF, in cooperation with the industry, to strengthen the use of DLT in the financial sector and, in cooperation with FINMA, to continuously review the legal framework with a view to making regulatory adjustments. *In this context, subject area leadership and active external communication on DLT in the financial sector are to be expanded in order to promote innovation domestically and attract innovation activities from abroad.* *In the area of the Collective Investment Schemes Act, the FDF/SIF, in cooperation with FINMA and the industry, is to examine which hurdles still exist concerning the use of blockchain and distributed ledger technology and, if necessary, prepare a proposal to remove them.*	- Active dialogue partner/coordinator and exploration of the topic for the financial market (ongoing) - If necessary, initiation of adjustment of the legal and supervisory framework (by 2025)
11 Green fintech	Continue to support efforts to make Switzerland a leading green fintech hub	The Federal Council instructs the FDF/SIF to actively introduce sustainable finance initiatives and green fintech as a topic in international bodies, and to seek dialogue with the relevant national and international players. *In particular, transparency and the availability of data in this area should be promoted. Relevant bodies include the G20 Sustainable Finance Working Group and the International Platform on Sustainable Finance.* *The FDF/SIF regularly informs the Federal Council about national and international work in the area of green fintech.*	- Active dialogue partner/coordinator (ongoing)
12 Potential for innovation	Strengthen the innovation potential of the financial sector in the long term by means of an innovation platform	The Federal Council instructs the FDF/SIF, in cooperation with the other bodies concerned and the industry, to submit a proposal to the Federal Council with specific objectives and a formal structure for an innovation platform for the financial sector.	- Preparation of proposal (2022)