Swiss Banking

Handling data in day-to-day business

May 2021

SBA guidelines

Executive summary

These guidelines explain some general principles of regulation concerning how data are processed and illustrate them using six different use cases from day-to-day banking business. The focus here is on the fundamentals of the revised Federal Act on Data Protection, the various forms of justification, technical and organisational measures (TOMs) and measures relating to the use of artificial intelligence (AI), in particular in the automated processing of personal data. The guidelines are intended primarily as an aid for SBA members to benefit safely from the opportunities presented by data processing.

- **Use of AI for compliance purposes:** Banks must assess the risk associated with using AI and should draw up a suitable use concept. In particular, they must document appropriate TOMs. Their choice of TOMs must be guided by the need to comply with the provisions on da-ta processing in the applicable data protection legislation.
- **Credit checks:** The data used must be complete and error-free, and their source must be clearly visible at all times. To ensure that only data of the highest quality are used and that data protection legislation is complied with, data for which the source is doubtful or cannot be verified must not be processed.
- **Trend analysis and benchmarking:** When personal data are anonymised, there is a residual risk of re-identification. Appropriate TOMs should ensure that re-identification is not possible. Analyses should be designed so that verifiable information on the composition of the data sets and the processing methods used can be provided when required.
- **Biometric authentication:** When assessing whether TOMs are appropriate, for instance with regard to data storage, due account must be taken of the fact that biometric data are sensitive personal data. Transparent communication about the use of biometric identification systems can make customers less reluctant to use them.
- **Personalised offers and advice:** Data may be analysed for this purpose at any time, provided the basic requirements are met, the analysis is carried out in good faith, and the data being analysed were supplied by the customer in the context of the bank’s typical activities.
- **Loyalty programmes:** Standardised customer loyalty programmes are unproblematic from a data protection perspective. However, customers must be informed about individually tailored programmes before joining. This information requirement can be waived if the customer was informed when entering into the business relationship.

1 Introduction

The use of data is becoming ever more important for the financial sector. Driven by technological progress, changing customer needs and regulatory requirements, views on how data can and should be used and what forms of processing are permissible will inevitably continue to evolve. By making efficient use of data, financial institutions can offer personalised products and services that are more relevant to their customers and ultimately provide them with better advice, while at the same time streamlining processes, reducing costs and improving risk management. Integrity and customers' trust are always top priorities for Swiss banks, and this means above all that they must be transparent as regards their data processing and the purposes it serves. When addressing the issue of responsible data handling, it is vital for the sector to take account not only of the regulatory and technical aspects (e.g. data security), but also of customers' views and expectations.

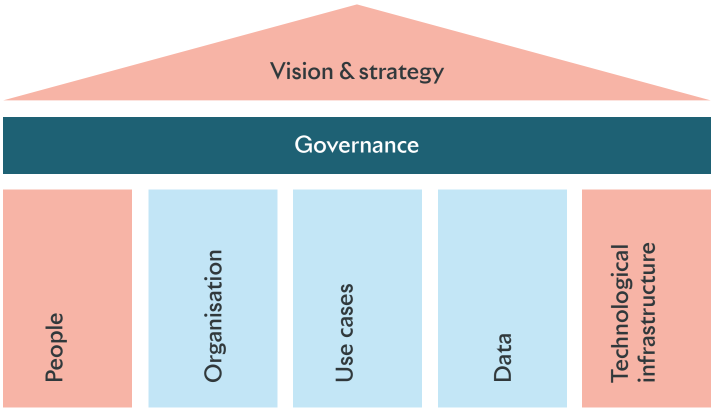
With this in mind, and with the revised Federal Act on Data Protection (revFADP) entering into force soon, a working group headed by the Swiss Bankers Association (SBA) has produced these guidelines. They outline six different practical use cases for data processing to help SBA members in their day-to-day handling of data. The guidelines are to be understood as an aid intended primarily for members rather than a legal or ethical policy. Use cases that already play a major role in everyday banking business today illustrate the principles discussed. This contrasts with other publications, which either take a holistic approach or set out a detailed code of conduct for a specific sector. The guidelines do not define sectorwide minimum standards, nor do they claim to be exhaustive. They will be periodically updated and expanded as necessary. Each individual financial institution is free to interpret and apply the content of this document in line with its own risk assessment.

Structure of the guidelines

The factors to consider when handling data as part of day-to-day business are described below on the basis of the framework shown in Figure 1. In addition to organisation, data and use cases, which constitute the main focus of these guidelines, a company's vision and strategy, how it treats its staff, cultural issues and its technological infrastructure are all key factors. However, since these are very specific to each institution and thus best addressed by the institutions themselves, they are discussed only peripherally or not at all here.

Figure 1

Framework of factors to consider when handling data



Source: SBA

The use cases were chosen with an emphasis on covering a broad cross-section of banking business. They are intended to aid the effective and targeted use of data to provide existing services for customers, create new ones or minimise risks[1]. The risks associated with the use cases should be assessed in line with the nature and quantity of the data processed and the form of processing. This risk assessment should be conducted as part of a bank's internal governance, and resulting decisions on business policies should be geared to upholding the principles of data protection legislation, such as purpose limitation, transparency, lawfulness and proportionality (e.g. in terms of data minimisation). Guidance on technical and organisational measures (TOMs) supports the correct and efficient implementation of the legal requirements (see section 2.4 below).

The bank's relationship with its customers must also be borne in mind. In this respect, the various means of informing customers can help to build trust. Each use case should be assessed to gauge whether there is a discrepancy between customers' expectations and the bank's actual activities. If there is, it should be eliminated, possibly by means of a privacy policy or other transparency measures. A bank's specific governance depends on its size, structure, complexity, business model and risks. This governance is a prerequisite for the use cases given here. Details considerations on the individual cases are set out as follows:

a. **Background:** introduction to the topic and added value for customers and the bank;

b. **Scope of application:** various examples for illustration purposes;

c. **Potential issues:** relevant issues and possible ways of solving them.

[1] The risks involved may be legal, reputational or operational.

2 Principles of data processing regulation

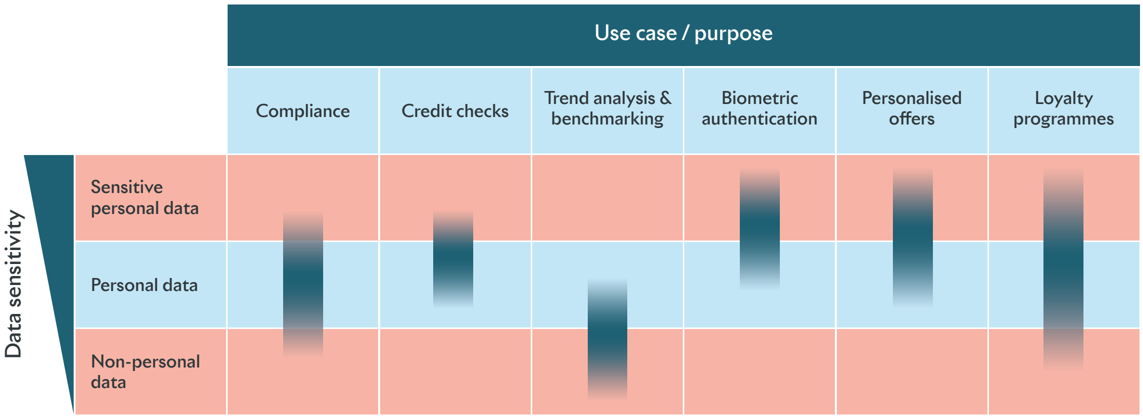
2.1 Handling data correctly

Regardless of the type of data being processed, the purpose of processing must always be borne in mind. Both the existing Federal Act on Data Protection and the revised version distinguish between the following general categories of data:

1. **Non-personal data**[2] **(not explicitly mentioned in the revFADP):** Data from which the identities of individuals cannot be deduced are defined as non-personal data. This definition includes anonymised data, which are logically not covered by the revFADP.
2. **Personal data (Art. 5 let. a revFADP):** This term covers all data relating to specific individuals, including data that can be attributed to specific individuals when combined or correlated with other data. These may be static data or data that allow conclusions to be drawn about an individual's behaviour, e.g. transaction data or geodata.
3. **Sensitive personal data (Art. 5 let. c revFADP):** This is an abstract subset of personal data defined precisely by law and including biometric data as well as information on religious and ideological views, private life and health[3].

Figure 2

Assessing the purpose of data processing and the sensitivity of the data



Source: SBA

[2] This is the term used by the European Commission.

[3] The complete list of sensitive personal data can be found in Art. 5 revFADP.

This three-way categorisation into non-personal data, personal data and sensitive personal data makes helps in assessing the sensitivity of each of the use cases outlined below. As will become clear, the legal status of data is not always easy to determine.

The sensitivity levels shown here are based on data protection law and do not necessarily correspond to the subjective sensitivity perceived by customers. Even within a category, it can make sense to apply differing degrees of stringency in accordance with the subjective sensitivity of the data and the associated risks. When handling bank customers' personal data, referred to by FIN-MA as client identifying data (CID)[4], bank-client confidentiality under Article 47 of the Banking Act (BA)[5] applies in addition to the provisions of data protection law. Over and above the confidentiality obligations set out in civil law, Article 47 makes violating bank-client confidentiality a criminal offence. With this in mind, FINMA has laid down specific technical and organisational requirements for handling electronic customer data[6]. Figure 2 should not be interpreted as an exhaustive illustration of the categories of data involved but as a general visualisation of the use cases outlined in section 3 below. The term "sensitivity" here is deliberately broad and intended to cover risks to a bank's reputation, perception by customers and the general public and ethical issues. In reality, every individual risk assessment conducted by a bank reflects the bank's specific risk appetite, so opinions with regard to sensitivity may differ.

Privacy Icons

Data subjects must be able to identify the ways in which their data are processed. This is normally achieved by means of a privacy policy, but it is not realistic to assume that everyone reads this thoroughly, if at all. Pictograms are a useful tool for making data processing more transparent. The Swiss association Privacy Icons (🔗 www.privacy-icons.ch/en/) offers a simple, easy-to-license solution. Various Swiss companies from a wide range of different industries have already implemented this solution or something similar.

[4] FINMA's definition of CID includes personal data of natural persons and the domiciliary companies, trusts etc. they own, referred to collectively as "private clients".

[5] Data of companies and other legal entities, i.e. including domiciliary companies and trusts, are no longer classed as personal data under the revFADP, provided they have no link to a specific individual. However, data of legal entities (including institutional customers) are in principle also subject to bank-client confidentiality.

[6] See in particular Annex 3 "Handling of electronic client data" of FINMA Circular 08/21 "operational risks – banks".

Open Banking and Open Finance

In a world where the value chain is becoming ever more fragmented, customers are increasingly receiving financial services from a wide range of providers such as banks, insurers, fintech companies and non-financial firms. The SBA has published a detailed overview of developments in this area. The most important point for the purpose of these guidelines is that this meshing of banks with other service providers entails sharing (customer) data.

There are a number of potential use cases for open banking and open finance in both the corporate and private customer segments, e.g.:

- **Improved liquidity planning** for business customers through integration of accounting software
- **Aggregating finances:** transparency with regard to business and private customers' financial situation through aggregation of various accounts and assets via a third-party provider
- **Payments:** straightforward, fast and secure transactions via an external provider

One thing these use cases share in common is that they involve customer data flowing between the bank and third-party providers. In this respect, banks need to ensure compliance with data protection law and bank-client confidentiality. Customers, for their part, must ask themselves what conditions should be attached to the bank sharing their data with third parties. The bank's duties in terms of monitoring and due diligence depend on the nature and intensity of its cooperation with third-party providers.

The cooperation and the flow of data between the customer, the bank and third parties must be clearly documented – in a contract where possible. It must also be borne in mind that open banking and open finance can involve two or more banks working together. Ultimately, transparency towards customers is the decisive factor. They must be informed as to which of their data are shared and what third parties do with them. The bank's business partners are not usually "real" third parties within the meaning of the revFADP, so the customer's prior consent is not typically needed to transfer data under an open finance arrangement. Prior consent is only an issue with "real" third parties due to bank-client confidentiality (see section 2.3 below).

https://www.swissbanking.ch/en/downloads

2.2 Profiling

According to Article 5 letters f and g of the revFADP, profiling is the automated processing of personal data for the purpose of evaluating specific personal aspects such as work performance, financial situation, health, preferences, location or mobility. Processing data – in particular determining correlations between data – makes it possible to analyse particular characteristics and behaviours of individuals or groups and predict them with a certain degree of accuracy.

"For financial service providers, high-risk profiling requires an assessment of the data protection implications."

For example, automated processing of payment data can be used to assess an individual's payment behaviour with a view to identifying anomalies immediately and thus preventing fraud by blocking suspicious payment orders to protect the customer and the bank (see sections 3.1 and 3.5 below). Profiling can also enable personalised, targeted marketing (see section 3.5 below).

These possibilities are also supported by the revFADP, which makes them all the more valuable. Profiling, for instance, can be performed on a group-wide basis without any extra requirements over and above those of bank-client confidentiality because group companies are not regarded as third parties under the Act (Art. 26 para. 3 and Art. 31 para 2 let. b revFADP).

The revFADP also introduces the new concept of "high-risk profiling" (Art. 5 let. g revFADP), which brings high risks to the privacy and fundamental rights of data subjects by linking data in a way that makes it possible to determine important aspects of an individual's personality. This definition essentially covers many elements that can be attributed to any kind of profiling and thus offers no clear distinction relative to "normal" profiling. The criteria for qualifying as high-risk profiling under Article 5 letter g of the revFADP need to be made more precise in practice.

For financial service providers, high-risk profiling requires an assessment of the data protection implications (see Art. 22 para. 1 and 2 revFADP). In addition, the risk of such data processing must be mitigated by means of customary technical and organisational measures (see section 2.4 below).

2.3 Forms of justification

In most cases, a bank can process data without its customers' consent. Swiss data protection law in principle permits the processing of personal data without the data subject's consent or any other justification if it does not violate or risk violating the data subject's privacy. The risk of violating privacy arises in particular when processing breaches the principles of data protection such as purpose limitation, transparency, lawfulness and proportionality (e.g. in terms of data minimisation). The specific forms of justification provided for by the revFADP are the data subject's consent, an overriding private or public interest and a legal obligation to process data.

The practical relevance of justification is explained below using two examples based on the principle of purpose limitation. A distinction must be drawn here between consent under contract law (in accordance with the Code of Obligations/CO), under criminal law (in connection with bank-client confidentiality) and under data protection law.

Where a bank collects customer data in order to fulfil its contractual obligations, it may only use such data for other purposes without the customer's consent if it has justification for doing so. Using the data to combat money laundering is permitted because this is a legal obligation on the part of the bank. As a rule, personal data can also be used to invite customers to an event without their consent because this is justified by an overriding private interest on the part of the bank. This contrasts with the principles of EU data protection law. Under the EU's General Data Protection Regulation (GDPR), any processing of personal data is deemed unlawful unless it meets the criteria stipulated for lawfulness.

In principle, the greater the risk to a data subject as a result of data processing, the more stringent the requirements for lawfulness. Where a customer's consent is required, a distinction can be made between two types of consent:

- **Implied consent:** Implied consent can be assumed in accordance with established legal principles, e.g. good faith (Art. 6 para. 2 and 3 revFADP), if the customer has been suitably informed and acts voluntarily. For example, if the customer is informed about new terms and conditions and fails to object to them before the stated deadline[7], implied consent can be assumed.
- **Express consent:** Express consent is only required where stipulated by the revFADP in accordance with Article 1 paragraph 2 of the Code of Obligations. It means that the customer must express consent directly, either verbally or with an appropriate sign. However, the revFADP's requirement for express consent does not follow the requirement for the written form under the CO. What is decisive under the revFADP is that the consent is given voluntarily on the basis of appropriate information on the subject of the consent, that it is unequivocal, and that it can be documented as evidence. Provided the contract is structured correctly and transparent information is provided, therefore, express consent may be given by accepting the general terms and conditions or simply by clicking on a button, for example.

However, the CO determines whether implied or express consent can be assumed in each individual case (Art. 1 para. 2 CO).

Banks must also check whether any requirement for consent over and above the revFADP applies. For example, bank-client confidentiality applies to bank customers' personal data. Some forms of processing require the customer to waive bank-client confidentiality so that data can be forwarded to third parties not acting as agents of the bank. Additional consent requirements may arise in connection with existing agreements between a bank and its customers.

Regardless of whether or not data processing is lawful, it can cause risks to the bank's reputation if there is a discrepancy between the processing the data subject may expect in good faith and that which is actually carried out. To avoid such discrepancies, a risk-review process should be established in which stakeholders of various kinds define a strategy for data processing that sets out which forms of

[7] If the customer must actively provide consent, this is often referred to as "opting in" – a very important term in the context of data protection law.

processing permitted by law are appropriate to safeguard the bank's reputation in line with its positioning on the market and which forms the bank should voluntarily forgo in the interests of its reputation.

2.4 Technical and organisational measures (TOMs)

Overview of TOMs

Experts identify the relevant legal requirements and draft practically oriented technical and organisational measures (TOMs) to ensure compliance with them. If technical measures prove ineffective or less effective than intended, organisational measures must compensate for this[8].

TOMs can thus account sufficiently for each bank's particular structure and processes. They are normally guided by expected levels of specialist knowledge, the technological state of the art, industry standards and best practice, meaning that they can change over time. TOMs must therefore be reviewed regularly to ensure that they remain appropriate and effective. This corresponds to the principles of "privacy by design" and "privacy by default" (see Art. 7 revFADP and Art. 25 GDPR), whereby TOMs must ensure that data processing complies in particular with the principles of purpose limitation, transparency, lawfulness and proportionality (e.g. in terms of data minimisation). This must be taken into account from the planning and design phase.

Examples of TOMs[9]:

- With regard to **confidentiality, integrity and availability**, FINMA's rules on operational risks and CID (FINMA Circular 08/21 "operational risks – banks" in particular Annex 3) and general ISO standards are useful references.
- For aspects such as **accuracy, purpose limitation, data minimisation** or **transparency**, it makes sense to draw up use concepts that define application-specific rules and controls for handling data.
- Rules on graphical user interfaces (GUIs), e.g. to govern **data processing** (purpose limitation, data minimisation) in connection with free text fields, may also be useful.
- The same is true for rules on **IT architecture** in general, e.g. with regard to **availability, resilience, capacity and proof of effectiveness** of IT systems and specifically for **technical interfaces** that define data exchange within a bank or with third parties in terms of data categories, purpose limitation, accuracy, data minimisation etc.
- Typical organisational measures that may be used to mitigate risks where suitable technical measures are lacking include rigorously function-based **assignment of data access rights, double-checking, restricting access to certain data** or **requiring prior permission** to process certain data.

[8] These guidelines only discuss selected TOMs. The Federal Data Protection and Information Commissioner (FDPIC) provides a detailed overview in the 🔗 Guide for technical and organizational measures.

[9] Further examples of TOMs can be found in the guidelines published by various IT service providers and supervisory authorities. However, these must be approached with caution as they often refer solely to the GDPR and EU law and thus do not take account of the significant differences in the overall legal framework and industry-specific rules in Switzerland. Such guidelines can nevertheless serve as a useful source of inspiration. The following are good examples: 🔗 Datenschutz Sachsen-Anhalt Checkliste TOMs nach DSGVO and 🔗 Das Standard-Datenschutzmodell (SDM) - ULD.

Specific examples of TOMs

Personal data are protected by adopting appropriate TOMs in (IT) security to ensure confidentiality, integrity and availability. These must not be confused with TOMs (which may be similar) in other areas of a bank's business that ensure compliance with bank-client confidentiality or data protection law, also known as the first line of defence. TOMs can serve, for example, to restrict or entirely rule out the identification of specific individuals by anonymising or pseudonymising data, meaning that the requirements of data protection law or bank-client confidentiality no longer apply.

The main technical options are currently as follows:

- **Anonymisation:** Anonymisation involves irreversibly and irrevocably changing certain personal attributes (e.g. a person's name or other identifiers) so that the data can no longer be linked to the data subject. From a data protection perspective, data are correctly and completely anonymised if the data subjects are neither identified nor identifiable, in which case the data unequivocally qualify as non-personal (see section 2.1 above).
- **Pseudonymisation:** In the case of pseudonymisation, personal attributes are not removed but hidden or replaced with pseudonyms, symbols or codes to ensure that the data can only be linked to the data subject using a special rule or key rather than directly. Data recipients can thus not be thought of as processing personal data unless they know the rule or possess the key. Pseudonymised data are therefore only anonymised from the data recipient's point of view. The data owner, meanwhile, can link data to individual data subjects because it knows the rule or possesses the key.
- **Encryption:** Encryption uses a key to convert personal data into an encoded text so that the original information can only be made readable again by using the correct key. Access to the key should be controlled by the bank and protected against unauthorised persons. The encryption procedure and the strength of the encryption key must meet current security standards for the encryption to be regarded as cryptographically secure. When CID are transferred, therefore, they should always be specially protected using suitable TOMs, e.g. encryption. In essence, encryption is a technical application of pseudonymisation rather than a separate concept in its own right.

2.5 AI – governance

Another topic set to warrant more and more attention from banks in relation to handling data is artificial intelligence (AI). The term was coined in 1956 during a conference at Dartmouth College[10]. The current AI boom has been fuelled by the increase in computing power over the past 15 years and the relatively easy availability of data for training self-learning algorithms. The various forms of AI are often categorised using the following hierarchy[11]:

- **Artificial intelligence:** AI is an interdisciplinary research field that aims to teach machines (computers) to behave intelligently.
- **Machine learning:** Machine learning is the use of algorithms to discover patterns in data. Methods employed include supervised learning, unsupervised learning and reinforcement learning.

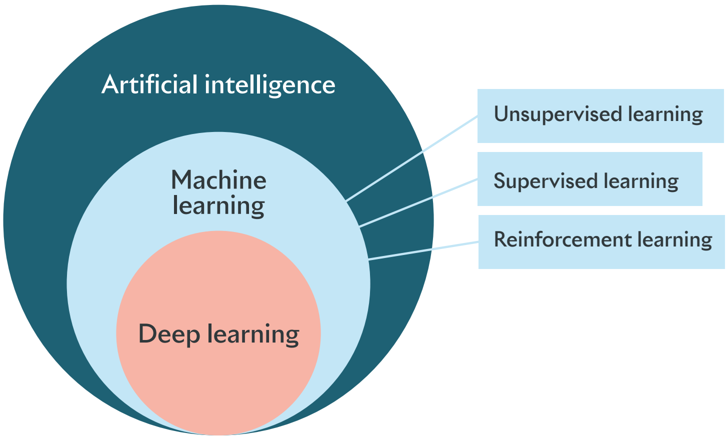
[10] See P. McCorduck (1979), "Machines Who Think".

[11] See T. Appenzeller (2017), "The AI revolution in science".

- **Deep learning:** Deep learning is a form of machine learning that enables computers to identify even more complex patterns (e.g. in unstructured data such as audio, video, still images or text). The "deep" part of the name comes from the multi-layered artificial neural networks employed.

Figure 3

Categories of artificial intelligence



Source: SBA, after the EU AI-HLEG

The key aspects to consider in relation to AI are as follows:

- the **quality and differentiation of the data sets used**, since undifferentiated or inaccurate data can yield discriminatory or incorrect results.
- AI-based **processes should be easy to explain, i.e. transparent and comprehensible.**
- **staff should be properly trained** to check that AI outcomes match the predefined parameters and take corrective action where needed.

Care must also be taken to check whether, in addition to the general duty to provide information under data protection law (Art. 19 f. revFADP), there is a further need for information on the nature of data processing by AI applications in the interests of customer trust and transparency. Providing such information could mitigate the associated risks to a bank's reputation.

For control reasons, bank staff are usually responsible for making decisions based on the outcomes of using AI. Where decisions are made entirely by AI systems without any intervention by staff, the potential legal consequences of automated individual decisions should be investigated and borne in mind (Art. 21 revFADP). If companies providing services to a bank gain access to and/or process personal data in connection with their use of AI systems, the provisions of data protection law concerning data processing by agents (e.g. Art. 9 revFADP) and possibly also the disclosure of personal data abroad

"For control reasons, bank staff are usually responsible for making decisions based on the out-comes of using AI."

(Art. 16 f. revFADP) must be observed. Under data protection law, agents are not regarded as "real" third parties pursuant to Article 31 paragraph 2 letter c of the revFADP, meaning that the customer's consent is not required for them to access sensitive personal data. In addition, the duty to provide data subjects with information is restricted (see Art. 20 para. 3 let. c point 2 revFADP).

Where service providers are contracted to process customer data, the legal requirements in respect of bank-client confidentiality (Art. 47 BA) must also be observed. The applicability of FINMA Circular 18/3 "Outsourcing" should also be investigated[12]. The SBA 🔗 Cloud Guidelines can also serve as a reference for assessing the requirements mentioned here as they contain details of the legally relevant aspects of sharing data with third parties (e.g. cloud providers).

Responsible AI

The use of new AI technologies can give rise to new risks such as bias, ethical issues, uncontrollable / inexplicable results ("black box" behaviour), a lack of robustness when exposed to new data and malicious attacks. A balance must therefore be struck between innovation and risk tolerance. A systematic approach to identifying, assessing, avoiding and controlling these risks is advisable. AI risk frameworks typically cover the following four areas:

1. **Governance** (e.g. IT governance, model governance, legal and compliance assessment, roles and responsibilities, ethics boards)
2. **Data management** (e.g. data protection, access rights, data quality, data control)
3. **AI principles, guidelines and codes of conduct** (e.g. explicability, fairness and equal treatment, transparency, ethics, security, controls, robustness and accountability)
4. **Communication, training and awareness** (e.g. peer reviews, staff training, using ethical trend radars to monitor the external image)

Responsible AI is an interdisciplinary research field encompassing technical, economical, legal, social and philosophical aspects, among others. Considerable advances have been made in all of these fields in recent years, e.g. as regards the explicability of algorithms, AI fairness, encryption and cryptography, and substantial further progress can be expected in the years ahead. At the same time, many governments, international standards bodies, companies and industry associations have drawn up their own principles and guidelines on the use of AI. An increasing number of initiatives are currently under way to flesh out these principles and guidelines and ensure that they can be put into practice. Given the fast pace of development in AI, the SBA advises bank staff who work with AI to keep themselves informed on an ongoing basis and to keep track of the latest research.

[12] If a service provider gains access to a significant quantity of customer data that qualifies as mass CID (FINMA Circular 08/21 "operational risks – banks", Annex 3, margin no. 53) in connection with machine learning systems, and the bank deems the service in question to be material.

3 Use cases

3.1 Using artificial intelligence for compliance purposes

Background

Banks continually analyse a wide range of customer data to combat money laundering and terrorist financing. Based on the statutory duties of due diligence, they gather, document and process personal data including names, dates of birth, contact details, copies of identification documents and, in some cases, information on the customer's financial situation as well as transaction data. The main source of such information remains the customer, but banks also obtain supporting data from various external sources such as the databases of specialised providers and the internet.

> "Combating money laundering and terrorist financing effectively is of crucial importance to the integrity of Switzerland's financial centre."

When processing data to combat money laundering and terrorist financing, banks can employ solutions based on artificial intelligence, and in particular machine learning (see section 2.5 above). The advantage of machine learning is that the system can teach itself to identify new risk areas and patterns of money laundering and terrorist financing. It also speeds up analyses, which can cover a range of data sources completely and in a uniform way. The aim of using such technologies is not usually to replace human decisionmaking, but rather to make the processes required by law more sustainable and efficient. The actual decisions are still taken by the bank employee responsible.

Combating money laundering and terrorist financing effectively is of crucial importance to the integrity of Switzerland's financial centre, and maintaining that good reputation is also key to Switzerland's international standing, for example within the Financial Action Task Force (FATF), which sets internationally agreed standards in this area and therefore serves primarily to protect bank customers. Such standards are the only way to ensure smooth settlement of international transactions.

Scope of application

Applications based on machine learning can be used at various stages in the customer life cycle:

- **KYC and onboarding:** Systems using AI can help to automatically identify the relevant data and compile risk reports during KYC processes and onboarding, by recognising individuals, places, facts and events and combining them using self-learned, dynamic patterns. They also filter and collate duplicated or similar information and flag potential risks. Efficient preparation of information needed to make decisions enables the bank's specialists to focus on the relevant sources and take reasoned decisions based on them.
- **Transaction monitoring:** Traditional transaction monitoring systems identify suspect elements solely on the basis of rules, using factors such as the value or frequency of transactions. Depending on the chosen threshold, this can lead to a higher incidence of false positive reports, unnecessarily increasing the number of cases that staff have to follow up, or a failure to identify risks at all if the threshold is too low. Machine learning systems recognise unusual changes in transaction volumes themselves, and link them in their analysis with other transaction monitoring criteria such as origin in a high-risk country,-

speed of asset movements, as well as sanction, PEP[13] and terrorism screening. This dynamic process has two major advantages: the analysis is more sophisticated and flexible than with traditional static systems, while cutting the number of false positives saves vital time in this area.

Potential issues
The bank should always examine the applicability of the criteria set out in section 2.5 when considering the use of AI. It should assess the risk associated with machine learning and develop a concept for its use. In particular, it should document which technical and/or organisational measures (TOMs) are appropriate in the given case, having particular regard to compliance with the processing principles contained in data protection legislation, such as purpose limitation, transparency, lawfulness and proportionality (e.g. when it comes to data minimisation) (see section 2.4 above). The risk associated with the type of data and how they are processed must also be taken into account, for example when dealing with sensitive personal data on administrative and criminal proceedings or sanctions, or when profiling – especially when high risks are involved (see sections 2.1 and 2.2 above).

The bank should also implement processes to ensure that the staff involved can monitor the correctness of the functionality or results and assess their plausibility (see section 2.5).

Note that the rule contained in Article 21 revFADP applies to fully automated individual decisions. This makes it especially sensible to implement processes that not only require staff to monitor systems but also give them decision-making powers (see sections 2.5 and 3.2).

3.2 Credit check

Background
Banks can used verified data to obtain information that allows them to correctly grade a customer's application for credit, identifying potential risks at an early stage and factoring them into the risk contribution[14]. This allows customers to receive personalised offers, improves risk management, and enables reserves to be planned and used in a more expeditious manner. With an eye to the rule on fully automated individual decisions contained in Article 21 revFADP, the comments that follow always envisage a human being taking the decision on whether or not to grant credit, i.e. the credit check process not being fully automated (see sections 2.5 and 3.1). In practice, this is a strategic decision taken by the financial institution concerned.

[13] PEP stands for "politically exposed person"

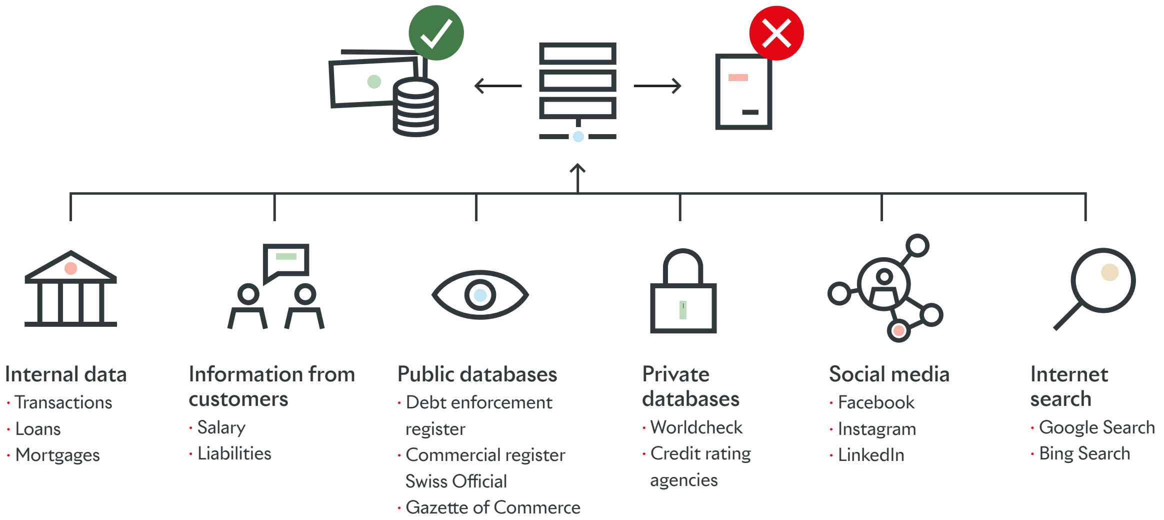
[14] Also based on historical customer behaviour data

Scope of application

Credit checks for both companies[15] and private individuals (applying for mortgages or consumer credit) rely on gathering data, but the way that is done depends on the use case. Where companies are concerned, much information is either in the public domain or can be easily obtained. With regard to private individuals, while the revFADP (Art. 31 para. 2 let. c) does not require consent to be obtained prior to extended data gathering from third parties, this may still be necessary owing to bank-client confidentiality. Rapid advances in technology now allow credit checks to be carried out very efficiently and largely by digital means using machine learning or natural language processing[16] (NLP).

Figure 4

Possible data sources (not an exhaustive list)



Source: SBA

Potential issues

There are a number of issues to be considered with regard to the data used for credit checks: they must be complete and error-free at all times; they should be up to date and correctly reflect reality; and their source must be clearly visible[17]. For data protection reasons, it is advisable not to use data in the credit check where there is doubt as to their source or it is not possible to verify them (this does not only apply to personal data). This is especially true when using social media and the internet as data sources. In general, it is advisable to communicate the quality of the data and their source transparently, verifiably and clearly. A precise description of the sources used may also be useful. Banks should additionally

[15] "Out of scope" under the revFADP.

[16] NLP is a form of AI that allows computers to understand natural language and so process and analyse large volumes of voice and text data. Typical applications include machine translation and speech recognition.

[17] Corresponds to the data protection law principles of lawfulness, correctness, up-to-dateness and transparency.

consider how they can best inform their customers in order to maintain their trust in the (partially) automated credit check and the confidentiality of their data at all times. TOMs must also be put in place to ensure that the use of external sources does not violate bank-client confidentiality, and that only data that are actually necessary are gathered, evaluated and used when taking the credit decision (see section 2.4 above).

In order to comply with the law while maintaining the trust of their customers (especially private clients), banks may need to obtain their express consent specifically for gathering data from external sources. The data gathered and used may also be disclosed, so that the rationale behind the credit decision is transparent and comprehensible. To best address the risks described in section 2, most data should be deleted if credit is refused, and only retained to document the basis for the decision if it is granted[18]. This protects the customer by requiring new, up-to-date information to be obtained if he/she submits a new application, rather than relying on historical data that may no longer be correct[19]. These approaches are already being used for corporate customers, though the processes employed are still largely manual. The main challenge in this case is, therefore, to automate the process as far as is sensible, i.e. in data sharing between banks, etc. and data staging[20].

3.3 Trend analysis and benchmarking

Background
Technological progress is accelerating changes in customer behaviour. The boundaries between markets are becoming increasingly blurred. Identifying and understanding customer needs and behavioural changes at an early stage is therefore a key success factor for banks. Trend analysis and benchmarking can be useful tools to this process. Banks must identify new trends quickly and understand where they stand in the market if they are to position their product portfolio optimally and align their sales strategies with it.

[18] The bank may have an overriding private interest in storing some of the data, for example to retain contact data and document the reasons for not granting credit.

[19] Here, the data protection law principles of correctness and up-to-dateness apply.

[20] Merging, cleansing and transforming data.

Scope of application

Banks hold large quantities of market, transaction and payment data that they can use in trend analysis and benchmarking for internal and external use:

Figure 5

Two examples from day-to-day banking business

EXAMPLE: TREND ANALYSIS (INTERNAL)

Product development and strategic marketing

Banks can use trend analysis internally to identify changes in customer/buying behaviour at an early stage (e.g. rising or falling demand for specific products, topics or sales channels, emergence of substitute products). Early-warning systems enable them to focus sales resources strategically and appeal to potential new customers. Trends and customer needs identified early can inform product development and result in product innovations (e.g. development of innovative ESG investment solutions).

EXAMPLE: BENCHMARKING (EXTERNAL)

Business insight tool in e-banking

Banks have valuable data on the Swiss corporate market in their possession. These can be anonymised, analysed and made available to customers, for instance in the form of a business insight tool containing aggregated data and benchmarking insights (e.g. an SME profitability comparison) based on data from various sources (such as transaction data, market data and public-domain sources). These benchmarks and reference data can be highly valuable for companies, helping them to improve their effectiveness and efficiency.

Source: SBA

Potential issues

Banks must establish which personal data they are able to use without further action and for which business areas – in other words, what is covered by their privacy policy and how TOMs can be used to comply with the processing principles (see section 2.4 above).

Processes such as anonymisation and aggregation of personal data involve a residual risk that individual, personal data can be made re-identifiable unintentionally. Appropriate TOMs should be implemented to ensure that personal data cannot be traced back to an individual or the identity of a customer inferred (e.g. via cross-analyses, random samples or combination with other data such as customer or public-domain data)[21].

[21] See in particular e.g. the EDPB guidelines dated 10 April 2014 (formerly WP29).

The level of aggregation or group size necessary to prevent linking to an individual must be determined on a case by case basis. Key criteria include the number of characteristics/attributes used, hierarchies and drilldowns, and the size and composition of the overall group. Additionally, only secure and effective methods of anonymisation based on current scientific methods[22] should be used, and analyses should only be performed by experienced specialists.

The data used may contain systematic errors (bias), for instance if a bank's customer portfolio is not representative of the Swiss population as a whole or the corporate landscape. There may also be spurious causal relationships, such as a statistical correlation between two variables without any actual causal connection. Current scientific findings, for example in the area of "algorithmic fairness", should be taken into account when handling data (see "Responsible AI" box, section 2.5 above).

Trend analysis and benchmarking should also be designed from the outset so that verifiable explanations can be provided if necessary and users are able to gauge the suitability of the results for specific issues and areas of application. It is advisable to provide brief, transparent information on the composition of the data sets and the methods used to process them in the context of the application.

3.4 Biometric authentication

Background
Biometric authentication methods such as fingerprint and facial recognition using a smartphone are proving increasingly popular, especially among digital-savvy bank customers, for whom security against forgery, uniqueness and, in particular, simplicity are the key issues. For the financial sector, they are a way to speed up and simplify processes at the customer interface and also a vital prerequisite for new, digital business models. Technical advances are also making new processes such as voice recognition appealing for banks. When used on the telephone, this can significantly increase both efficiency and convenience for customers, who are no longer required to answer questions in order to authenticate themselves. The customer's voice is compared with the stored profile while he or she is talking, and once a match has been obtained, the bank employee can proceed directly to dealing with the subject of the call.

Generally speaking, biometric attributes cannot be changed and can therefore always be matched to a specific individual[23].

[22] Examples of anonymisation technologies and anonymity and security measures include k-anonymity, l-diversity, t-closeness, anatomy, differential privacy and the use of synthetic data.

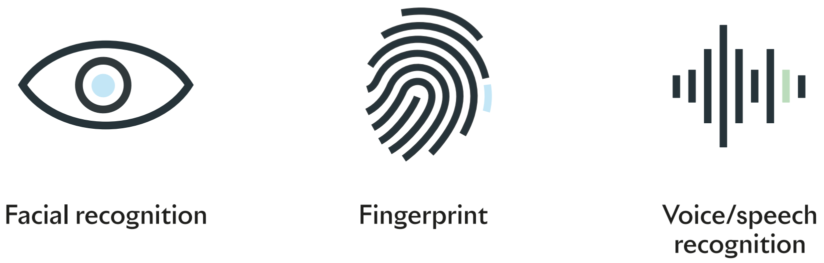
[23] The comments in this section are restricted to three methods: fingerprint, facial recognition and voice/speech recognition.

Scope of application

Biometric authentication can be used in many areas of day-to-day banking. The most appropriate method will depend on the nature of the interaction.

Figure 6

Biometric authentication methods in day-to-day banking business



Source: SBA

Typically, customers will specify once which method of authentication they wish to use to log in to mobile or e-banking and for telephone calls. Purely digital authentication generally produces very good results[24].

Potential issues

The basic distinction is between fingerprint, facial and voice recognition. When using fingerprint and facial recognition, the bank often does not store any data. Currently, the procedure takes place on the customer's own mobile phone, so that the bank is not responsible for complying with data protection legislation. In both cases, the revFADP requires transparency, for example in the form of a privacy policy, but not consent. Voice recognition is different, because the voiceprint, which constitutes biometric data, is held either by the bank on its own premises or at a location in the cloud[25] for which it is responsible. Consequently, the relevant provisions of the revFADP apply.

Generally speaking, storage of biometric data (technology, server location) is subject to compliance with data protection law covering, for example, the data subject's right to view or correct his or her data, deactivate biometric authentication where it has been activated, and delete the relevant data.

[24] See also FINMA Circular 16/7 "Video and online identification".

[25] See SBA Cloud Guidelines.

A biometric profile can also be used to determine other characteristics such as age, gender and even current state of mind. The ways in which the profile is to be used as a means of identification must therefore be specified in full, and no other use can normally be permitted without additional consent from the customer (Art. 6 para. 3 revFADP). Exceptions may only be made to this rule (for the purposes of criminal prosecution, for example) if the law provides for them (e.g. Art 31 para. 1 revFADP, see also section 2 above.

“Customer identification is of course subject not only to data protection law but also to compliance with the rules on bank-client confidentiality.”

Customer identification is of course subject not only to data protection law but also to compliance with the rules on bank-client confidentiality. FINMA therefore issued specific rules on handling client identifying data (CID) in its Circular 08/21 “operational risks – banks” and in particular Annex 3. As mentioned, it contains TOM requirements by means of which banks can comply with their duty to ensure the confidential-ity of CID in a digital world.

Transparent communication about the use of biometric identification systems can make custom-ers less reluctant to use them and also mitigate potential reputational risks. From the customer’s perspective, convenience is also a factor in favour of consenting to biometric authentication, alt-hough such consent is not a legal requirement.

3.5 Personalised offers and advice

Background
Banks want to offer every customer a comprehensive range of products and services geared to their individual needs, based on the best possible data, including targeted advice if they so wish. The range should reflect the customer’s known interests and values, such as sustainability. The composition of the offering is not tied to a particular channel, and should allow for material changes in the customer’s circumstances – resulting from marriage, divorce, the birth of children, inheritance, change of job and retirement, for instance – to be identified as early and systematically as possible. Such events typically lead to changes in customers’ banking needs. It should be remembered, however, that they may also affect third parties, such as the customer’s spouse, whose data are also protected and who may, if they are additionally customers of the bank, enjoy the protection of bank-client confidentiality. Where necessary, they should be involved transparently in the process, for example via the customer.

Data gathering can be fully automated or – in principle – fully manual. However, digital solutions allow the bank to serve customers more comprehensively, efficiently and appropriately, and offer the same standard of quality to all. The more extensive the data sets used, the better the quality of the offering and the more precisely it can be targeted. Automated data gathering combined with a personalised offering also allows for a truly customer-centred advice service.

Scope of application
Specific offerings can be triggered when they are most appropriate: a mortgage offer, for example, is best sent out shortly before an existing fixed-term mortgage expires and not when the bank decides to

roll out a nationwide mortgage campaign for all customers, regardless of their needs. Systematically gathered data on customer preferences can be used to target them with personalised marketing for new bank products or services, such as a newly launched investment vehicle. Analysis results can also feed into direct advisory services such as a structured investment advice agreement based on the finding that, for example, the customer prefers direct investments over fund solutions or wants to focus on sustainable investments. Structured knowledge of customers, their preferences, values and personal circumstances allows them to receive the service best tailored to their needs. As well as enabling cross-sales, analysis results allow the bank to protect customers' interests by monitoring their payment transactions for anomalies (see sections 3.1 and 3.3 above). They can also be used in anonymised form for statistical or strategic purposes (see section 2.4 above).

"The more extensive the data sets used, the better the quality of the offering and the more precisely it can be targeted."

Potential issues

One potential issue concerns what data the bank wants and is permitted to analyse, and about which business areas, without first obtaining the customer's consent (transparency will suffice). This will depend on the quality of the data and the particular circumstances (see section 2 above).

The bank may have access to customer data that were not obtained during the original bank activity, for example when providing tax advice. For this reason, many customers deliberately choose to obtain such services from another bank, for reasons of discretion.

The question is whether and under what circumstances those data can be used for personalised offerings. While the bank may regard an approach as sensible and very much in the customer's interest, the customer may take the opposite view. Unsolicited offerings can be seen as a nuisance and undermine the customer's trust in the bank's data processing activities generally.

Data analysis and personalised marketing based on it is always permitted without further action, provided the basic requirements set out in section 2.3 above are met and the analysis is carried out in good faith[26], as long as all of the following apply:

- The analysis is based on data supplied by the customer. Data obtained from third parties with the customer's knowledge are to be treated in the same way.
- The data were obtained by the bank in the context of its typical activities. The latter will depend on the bank's business model: in the case of a full-service bank, for example, they will include account, payment, financing and investment services.

Where the data are obtained by the bank in the context of activities that are not typical, such as inheritance or tax advice, the bank must assess whether transparency is needed before they are used

[26] Art 5 para. 2 revFADP explicitly enshrines the principle of good faith in data protection law.

for other purposes within the scope of typical activities. This caveat derives not just from the good faith principle but also from the requirements under data protection law regarding purpose limitation and proportionality of data processing (see Art. 6 para. 2 and para. 3 revFADP). If a cus-tomer states that they no longer wish to receive personalised offerings either generally or in spe-cific areas, the bank must implement this, which is easier to do in a digital system than in a purely manual one. In this context, fully digital data gathering may qualify as profiling, depending on whether the data are normal or high risk in terms of sensitivity (see section 2.2 above). Subject to the general requirements, data gathering from third parties does not require the customer's specif-ic prior consent if the data concerned are deemed in good faith to fall within the customer's experi-ence and expectations (see section 2.3 above).

When active on social media, bank staff such as customer advisors must, in addition to complying with the law, adhere to the bank's own rules on accessing and using social media and the data located there.

3.6 Loyalty programmes

Background
Loyalty programmes have a positive influence on customers' attitudes and buying behaviour and tie them more strongly to the bank. They are also a way for banks to differentiate themselves.

In these guidelines, the term is used for programmes implemented by banks using customers' personal data (such as payments) to gear them to individual preferences.

It does not include indiscriminate "rewards" offered equally to all customers, such as a CHF 20 voucher every time they open an account, since these do not require the processing of personal data.

Scope of application
Loyalty programmes can broadly be classified as follows:

1. **Cashback:** Bank customers earn discounts on the range of brands that match their interests on the basis of financial (e.g. credit card) transactions with the bank. The bank credits the discount to the customer's account after the purchase has been made, and at the same time obtains information from the purchase about the customer's personal preference.
2. **Points system with personalised advertising:** Customers earn points by carrying out financial (e.g. credit card) transactions with the bank. They can then use the points to select products from a catalogue that in most cases have nothing to do with the bank. The offers are available to all, but the advertising is personalised by evaluating personal data – deducing purchasing behaviour from transaction data, for example.
3. **New business:** Loyalty programmes can also provide an incentive for existing customers to use additional services. For example, a customer can accumulate points for credit card transactions or trading activity and exchange them for lower interest on a new mortgage or higher interest when opening a savings account.

The first two types of programme involve banks using customer data that they already hold internally, but potentially sharing personal data with third parties.

Potential issues

Standardised loyalty programmes are fairly unproblematic from a data protection perspective.

The individually tailored programmes described above, however, may gather and use static data (e.g. last name, first name, sex, address, telephone numbers, age, size of household, job, educational qualifications, card number, payment methods and data) and geodata (e.g. place of residence, distance from nearest company location).

Using such data for personalised marketing of third-party products is no longer part of processing the general banking relationship and is therefore beyond the scope of the purposes for which the customer originally supplied them. In this case, customers must be fully informed before joining the programme[27].

“Loyalty programmes can add value for both the customer and the bank.”

This information requirement can be waived if the customer was informed when entering into the relationship that data would be shared with third parties for the purpose of personalised advertising of third-party products. Data must also be processed in accordance with the law and in good faith (see section 2.3 above), and for a specific, identifiable purpose, in this case the administration of loyalty programmes.

Loyalty programmes can add value for both the customer and the bank. The data that banks gather contain information that is also of value to third parties. In today’s world, where data may be commercialised outside the financial sector, it is entirely possible that customers will be sceptical about loyalty programmes, because they suspect their personal data may be shared with third parties.

Clear communication about sharing of customer data with third parties can help to dispel concerns and create trust – especially if no data are in fact shared in this way. Banks should establish whether data protection law or at least bank-client confidentiality (Art. 47 BA) requires them to obtain the customer’s prior consent, and consult FINMA Circular 08/21 “operational risks – banks”, Annex 3, for specific details relating to the handling of electronic data.

[27] For example by means of a clear reference, when the business relationship is entered into, to information about the programme that can be easily found on the website.

Swiss Bankers Association
Aeschenplatz 7
CH-4002 Basel
office@sba.ch
www.swissbanking.ch