Navigating AI with Pestalozzi – Part 4: Data Protection

24.10.2024

Key Takeaways

- **The processing of personal data by companies operating in Switzerland – also in context of AI applications used by such companies and individuals – must comply with all applicable data protection laws.**
- **Many aspects to consider from a data protection perspective are not particular to AI applications. Given the amount of potential personal data involved, however, the AI context increases the relevance of data protection law.**
- **Besides technical measures, when it comes to data protection, the proper training and inclusion of employees in AI projects are essential.**

Introduction

With the rapid advance of digitalization in recent years also came an increase in digitally available data. Thanks to "Big Data" technologies, the analysis of data previously limited to a company's own data warehouse can now be expanded to almost infinite amounts of data from an almost infinite number of sources.

When faced with this data abundance, many companies fall back on AI to improve efficiency: AI's machine learning capabilities make it easier to process massive and highly complex datasets, identify patterns, develop detailed insights, and filter out very particular information from deep inside the ocean of Big Data. Thus, companies believe that these solutions will allow them to make faster and more accurate decisions, anticipate market and industry trends, analyze customer behavior, optimize, and personalize digital marketing as well as raise their business performance and efficiency overall to carve out a competitive edge.

The processed data often includes "personal data", meaning any data referring to identifiable individuals (the "data subjects"). Some examples of personal data are a person's name, address,

date of birth, sex, gender, telephone number, bank account details, IP address, license plate number, and location data.

In this context, the processing of such personal data – meaning any relevant handling of data, including the training, fine-tuning, or prompting of the AI – regularly raises questions and concerns about data protection. It remains, however, important to remember that not every type of data automatically is personal data and, hence, there may be certain AI applications or processing activities that do not fall under data protection legislation. The latter may be the case where such AI applications only process factual data or anonymized or (arguably) pseudonymized data. While this delineation will continue to be discussed and developed, the focus of this contribution lies on solutions that process personal data, for example, in the context of the input received or the output created and used.

Most companies in Switzerland process large quantities of personal data on a regular basis, and with the introduction of AI applications this amount will only increase. It is therefore crucial to understand what risks are associated with the use of AI in terms of data protection and how a company can appropriately avoid and/or manage these risks. While many data protection pitfalls arise irrespective of AI, some are more prominently connected to its deployment.

Data Protection Checklist for the Use of AI

If a company chooses an AI application, either internally as an "auxiliary" for employees (e.g., ChatGPT) or externally as a tool in customer service (e.g., digital sales assistant chatbots on a company's website), the company bears responsibility to ensure data protection. For Swiss companies operating beyond Swiss borders and processing the personal data of natural persons outside of Switzerland, in addition to Swiss data protection laws, other data protection laws may apply (e.g., the data protection laws of the EU).

Especially, the deployment of a sales assistant chatbot may involve extensive collecting and processing of personal data, as the AI application relies on personal data to effectively work, understand what the customer wants, and, thus, answer requests or make targeted offers. A chatbot may not only receive information on, for example, age, gender, or addresses, but beyond such basic information potentially also personal preferences and users' moods and any other piece of information a user decides to share with such chatbots.

The following set of questions intend to help a company avoid and/or manage data protection risks with a particular focus on AI.

Question 1: Do you inform your employees and customers that their data is being processed?

Data subjects, such as employees and customers, have a right to be informed about the processing of their personal data, irrespective of whether this data is processed in context of AI. Usually this is done in the form of a privacy notice. As a minimum, a privacy notice must include (1) the company's identity and contact details; (2) the purpose of the processing; (3) where applicable, the recipients or categories of recipients to whom the personal data are disclosed; and (4) if the personal data are disclosed abroad, the country and, if such country does not provide for an adequate level of data protection, the guarantees taken to ensure their data protection, or the exception relied upon.

The company must inform the data subject regarding the processing of personal data both in cases in which AI applications are used by employees to process personal data as well as in cases in which the data subject themselves, as customers, use an AI application provided by the company. The law does not contain any explicit provision on any information obligation regarding the use of an AI application. Since customers, however, may not always recognize that their personal data is being processed by AI, for example, when chatting with a chatbot, the company is well advised to inform their customers that they are chatting with AI and not another human being.

Question 2: Does the AI application make automated decisions? If so, do you inform your employees and customers about this fact?

Certain AI applications may offer functions that qualify as automated decision making; for example, if a chatbot only grants relevant discounts or benefits to certain customers or presents different contract conditions based on the AI application's analysis. In such cases – in addition to its general information obligation – the company must inform the data subject about the fact, that a decision was made based solely on automated processing. This information is usually also included in the privacy notice. The data subject has the right to request the review of this automated decision by a human being.

Question 3: Did you implement a record of processing activities, or did you update your record of processing activities?

If your company (1) has a total of 250 employees or more, (2) processes large amounts of sensitive personal data (such as data on ethnicity, origin, and race, religious beliefs, political opinions, sexual orientation, health, biometric or genetic data), or (3) engages in high-risk profiling activities, your company is required to list all data processing activities in a so-called "record of processing activities". Thus, even if your company has less than 250 employees and has, so far, not been subject to the obligation to have in place this record, the necessity for implementing of this sort of record might arise due to the deployment of an AI application. Whether this is the case, must be decided on a case-by-case basis and ultimately depends on the functionalities of the AI application.

Question 4: Did you carry out a data protection impact assessment ("DPIA") before deploying your AI application?

Companies must carry out a DPIA if a planned data processing activity is likely to result in a high risk to the data subjects' personality rights. A high risk may, especially, arise in context of new technologies. A DPIA is thus a critical – and mandatory – self-assessment tool for companies when deploying an AI application, like a chatbot. If it follows from the DPIA that the risks of the planned data processing activity are, indeed, high, the data protection authority must be informed, unless the company has appointed a data protection officer and consulted them as part of the DPIA.

Question 5: Is your role and the role of the AI provider clearly defined in terms of data protection?

If your company obtains AI as a service from an AI provider, you will likely assume the role of a controller, i.e., the person who determines the purposes and means of the data processing. The AI provider, on the other hand, will likely – and at least to a large part – assume the role of a processor, i.e., the person who carries out the data processing on behalf of the controller.

As the data controller, the company must ensure that the AI provider, as the data processor, processes the personal data in compliance with data protection laws and according to the company's instructions. In particular, the company must oblige the AI provider to ensure data security. Therefore, it is mandatory by law that the company enters a so-called "data processing agreement" with the AI provider. This agreement should include provisions on the technical and organizational measures that this AI provider must take to ensure data security. In practice, this data processing agreement will likely be included in the general terms and conditions of the AI provider.

Question 6: Is the AI provider located outside of Switzerland/the EEA/the UK?

Where the processing of personal data is transferred to a processor located outside of Switzerland, the company must assess whether this processing occurs in a country that, according to the Federal Council's decision, provides for an adequate level of data protection. This can generally be assumed for the countries in the EEA and the UK. If this is not the case, the company must ensure an adequate level of data protection through other measures. The most common way is by entering into the EU Standard Contractual Clauses ("SCCs") – a legal framework that can be included as an annex to the data processing agreement. Additional analysis on the effectiveness of those SCCs in foreign jurisdictions may be needed.

Question 7: Do you apply appropriate data security measures?

AI applications are usually not isolated from your overall IT system. To comply with your data security obligations, appropriate technical and organizational measures must be taken to protect personal data against any data security breach. We suggest regularly testing the security of your systems. For this purpose, ensure that your servers and anti-virus software are up to date, perform regular penetration testing, and fix existing security vulnerabilities as soon as possible – the same as you would for your other IT systems. As many data breaches can be attributed to weak or stolen passwords, ensure that your employees use strong passwords and do not leave their computers unlocked when unattended, especially when working remotely, as well as enforce two-factor authentication. Wherever feasible for the use case, personal data should be anonymized, pseudonymized, or encrypted.

Question 8: Do you know how to react in the event of a data breach?

With a data security breach – for example, a cyber-attack that leads to the loss of personal data – a company is obliged to notify the data protection authority of this incident, provided that such a data security breach results in a high risk for the personality of the affected data subjects. Moreover, a company is obliged to inform the affected data subjects of this breach if it is necessary to protect the affected data subjects (e.g., they must change their passwords) or if the data protection authority requires it. Given that through AI applications, specifically with chatbots, potentially large amounts of customers' personal data are collected and processed, it is not unlikely that the loss of such data would meet the threshold of "high risk" and a notification obligation may arise. If an obligation arises, the company must inform the data protection authority as soon as possible. Needless to say, in case of a data breach, mitigating measures should be deployed wherever possible.

Question 9: Are you able to answer a request for information? Are you able to provide sufficient information on the logic of the AI's decision making?

If an employee or customer requests information from the company as to whether personal data relating to them is being processed, the company must be able to provide such information within 30 days. As a minimum, the company must inform them about (1) the identity and contact details of the company, (2) the processed personal data as such, (3) the purpose of the processing, (4) the retention period of personal data, (5) where applicable, the recipients or categories of recipients to whom personal data are disclosed, and (6) if the personal data are disclosed abroad, the country and, if such country does not provide for an adequate level of data protection, the guarantees taken to ensure such data protection, or the exception relied on.

On top of the above – which is specific to AI applications subject to automated decision-making – an employee or customer also has a right to obtain information regarding the reasons for the AI application's decision allowing them to comprehend and review the AI decision. The company must therefore provide the data subject with information on the decision-making criteria and personal data which the decision was based on. In practice, this can be a major challenge for a company due to the black-box nature of many AI applications. In many cases, the company will be dependent on the cooperation of the AI provider to acquire the necessary information to fulfil its information obligations under data protection law. This

should be taken into account when concluding the contract with the AI provider.

Question 10: Do you ensure that only data is collected that is necessary to achieve the communicated purpose?

To analyze customers' personalities and purchasing behaviors, companies have an interest in collecting as many personal characteristics about their customers as possible. However, when processing personal data, they are bound by the principles of proportionality and purpose limitation. Following these principles, the collection of personal data must be minimized to such personal data that is required to achieve the intended purpose(s) of the processing. The company must therefore – before collecting such data – assess which personal data is necessary for a specific processing purpose (e.g., marketing activities).

It goes without saying that in context of AI applications, such as a chatbot, companies will often not be able to fully control the personal data the AI processes, since it is the customer as user of the AI application who decides what personal data they share with the AI application. It is therefore advisable to request your customers limit the personal data they provide to the extent required as well as regularly audit customers' data storage and delete personal data that is no (longer) needed.

Question 11: Do you spread awareness on data protection among your staff?

It is crucial to properly instruct and train employees to treat their own personal data and the personal data of their co-employees and customers with the appropriate care and in compliance with data protection laws. Employees should be trained to be careful with the information they use as an input for the AI application and to avoid using personal data whenever possible. Sensitive personal data should not be used at all unless the concerned data subject has given its consent to do so. Wherever possible, employees should only rely on anonymized data (i.e., data changed so that it can no longer be traced back to the data subject) or pseudonymized data (i.e., data encrypted so that only authorized people with access to the encryption key have access). As regards the output of an AI application, employees should carefully review if such output contains personal data, and if so, remove them before using the output, unless the concerned data subject has given its consent to do so. In any case, employees should ensure that the personal data contained in the output is correct.

Question 12: Is there anything else you can do to strengthen data protection in your company?

Appointing a data protection officer would be a useful asset for the company when it comes to data protection governance in the context of critical data processing activities involving AI. A data protection officer serves as a first point of contact for data subjects and authorities and takes over the important task of training and advising the company and its employees in data protection matters.

Last, it is generally recommended to establish internal processes, data protection policies, and action plans to ensure compliance with data protection requirements, particularly around the internal use of AI applications. On the technological level, IT solutions can be implemented for

the controlled deletion of personal data when it is no longer needed, reducing the risk of data breaches, and simplifying compliance. In the event of a data breach, action plans with clear step-by-step instructions, and checklists come in handy.

Through a combination of the above outlined measures, companies can adequately respond to data protection hazards and manage risks in connection with the deployment of AI-based applications such as chatbots. On top of that, having appropriate data protection governance in place will not only limit the risk for (data protection) liability, but also strengthen the trust of clients, customers, and other stakeholders, resulting eventually in a competitive advantage on the market.

Contributors: Sarah Drukarch (Partner), Markus Winkler (Counsel), Carola Winzeler (Associate), Valerie Bühlmann (Junior Associate)

No legal or tax advice

This legal update provides a high-level overview and does not claim to be comprehensive. It does not represent legal or tax advice. If you have any questions relating to this legal update or would like to have advice concerning your particular circumstances, please get in touch with your contact at Pestalozzi Attorneys at Law Ltd. or one of the contact persons mentioned in this legal update.

Sarah Drukarch

Partner
Attorney at Law

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 93 23
sarah.drukarch@pestalozzilaw.com

Michèle Burnier

Partner
Attorney at law

Pestalozzi Attorneys at Law Ltd
Cours de Rive 13
1204 Geneva
Switzerland
T +41 22 999 96 00
michele.burnier@pestalozzilaw.com

Markus Winkler

Counsel
Attorney at law, Dr. iur., Dr. sc. math. ETH

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 92 59
markus.winkler@pestalozzilaw.com