Diarienummer:
IMY-2023-2602

Datum:
2023-03-15

English Summary: Swedish Authority for Privacy Protection, IMY, finishes first Sandbox Pilot

• Introduction: Complex societal challenges require innovative solutions. Sweden and the EU face a number of societal challenges for which innovation and new technology can offer new, more efficient solutions. Today's innovation system has a strong drive to develop sustainable solutions, but there is oftentimes uncertainty as to how data protection regulation should be applied to new technologies. For legislators and authorities interpreting and applying the regulations, it is a challenge to understand and analyse the new technologies to which the rules will apply.

• There is a risk of an increasing gap between the rapid development of technology and the lengthier work of developing, interpreting and applying regulations. Developing new ways of working in the public sector is an important part of the way forward. One of the working methods often discussed in this context is regulatory testing activities, often referred to as 'sandboxes'. There is no generally accepted definition of this approach, but the essence of the idea is that innovators and regulators work together to interpret how regulations can work in practice with innovative products and services.

• During the autumn of 2022, the Swedish Authority for Privacy Protection, IMY, conducted our first pilot with a regulatory sandbox. IMY's approach to a regulatory sandbox is that we provide in-depth guidance to a specific innovation initiative on how the data protection legislation should be interpreted and applied. A characteristic of the approach is that IMY, together with the participants, identifies the legal issues that the guidance should focus on. Guidance is then given on several occasions over a few months, in the form of workshops or other dialogue-based formats. The work results in a public report where reasoning and assessments are summarized to enable learning for a broader audience.

• The project *Decentralized AI in Health Care: Federated machine learning between two healthcare providers* was IMY's first pilot with a regulatory sandbox. In the pilot, two healthcare providers, Region Halland and Sahlgrenska University Hospital, wanted to evaluate the possibilities of jointly training and exchanging machine learning models. The work is supported by AI Sweden, the national center for applied AI. Information-driven health care, which to an increasing extent uses AI, can contribute to decisions being tailored at the individual and system level to develop more advanced and accurate diagnoses and treatments. The aim of this specific project, was to better predict the re-admission of heart failure patients within 30 days of the last hospital stay, using federated machine learning.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

• **Federated machine learning involves multiple parties jointly training a machine learning model without collecting data centrally.** The technology is the most common form of decentralized AI, which is a new paradigm in machine learning. In short, the principle underpinning this technology is that each party trains a local machine learning model using their own data. In the next step, the lessons learned are combined to a common machine learning model.
The training is thereafter repeated on the local data. One reason to use federated machine learning may be that the parties, individually, have insufficient training data. When developing federated machine learning, the basic goal is that there should be no transfer of personal data between the parties.

• **The guidance in the pilot project has focused on three legal issues** that Region Halland, Sahlgrenska University Hospital, AI Sweden and IMY jointly selected. It should be noted that there are additional legal issues that need to be analyzed for data protection compliance, but not were addressed within this particular sandbox. For example, the sandbox discussions did not address how the data subjects' right to information or the principle of data minimisation is to be met. The issues discussed were:

• **Q1. Is there a legal basis for the processing of local personal data, i.e. when healthcare providers train the machine learning model locally, solely on their own patient data?** IMY's assessment is that there appears to be a legal basis for the local personal data processing. Key in this context is that IMY advocates a dynamic and technology-neutral interpretation of the purpose provisions found in the Swedish Patient Data Act and the Health Care Act. This means that what fits within these provisions may change over time, among other things, considering the development of technology.

• **Q2. In the case of federated machine learning, is there a disclosure of personal data between the healthcare providers?** Using intentional, invasive methods, such as the Membership Inference Attack or Model Inversion Attack methods, it would be possible, albeit cumbersome, for Region Halland or Sahlgrenska University Hospital to obtain personal data from the other party. IMY's assessment is therefore that Region Halland and Sahlgrenska University Hospital would be disclosing personal data to the other party, while combining the lessons learned from the local training into a common machine learning model. However, this does not mean that the same conclusion can be applied to other forms of federated machine learning.

• **Q3. Is there a legal basis for the disclosure of personal data between healthcare providers?** IMY’s assessment was that if Region Halland and Sahlgrenska University Hospital, which are both government authorities, were to request patient data from each other under the Public Access to Information and Secrecy Act, disclosure could possibly be allowed provided that the information is not secret. In general, however, patient data in healthcare is secret. IMY has not assessed whether any provision that overrides secrecy could be applicable in the present case.

• **Cross-functional work is essential to successfully drive innovation while ensuring good data protection.** Based on the pilot project, IMY made some general reflections regarding the necessity of cross-functional work in innovation processes. In order to be able to make relevant legal assessments, a relatively deep understanding of the technology is required from the lawyers involved. Good pedagogical skills are

therefore essential, both from technicians and lawyers. Different structures and tools can facilitate building a common understanding in the team. It can also be helpful to continuously go back to, and if necessary revise, the legal question being investigated, since deepening understanding of the technology can lead to new or modified questions.

• **IMY's assessment is that regulatory sandbox is a beneficial way of working, creating value and learning** both for the organizations in question and for the supervisory authority. Region Halland, Sahlgrenska University Hospital and AI Sweden state that they have received valuable guidance, through the questions asked by IMY and the assessments made. For IMY, the pilot led to increased understanding of federated machine learning and the legal issues and challenges. IMY intends to carry out a second pilot with a regulatory sandbox in 2023.