



PRIVACY ASPECTS OF FEDML

# Legal Opinion by CMS



## A. Brief introduction to Federated Machine Learning

„Machine Learning“ describes a process in which an algorithm uses data to train a model („Client Model“). This model may then be used by XAIN’s „Clients“ to make decisions or predictions which are not programmed in the algorithm itself, but which are solely based on the model. A Machine Learning model is typically only a vector of parameters of a mathematical function which provides a result  $y$  for given value  $x$ .

**Example:** A very simple model might look as follows:  $(x_1, x_2) = (1.45, 5.34)$ . This simple model could be used in the algorithm  $y = 1.45x_1 + 5.34x_2$ , which „predicts“ the result  $y$  for a given  $x = (x_1, x_2)$ .

In practice, Machine Learning models consists of hundreds of thousands of parameters.

In „Federated Machine Learning“, a company running a parameter server is collecting the trained Client Models from various clients, aggregates such Local Models to one aggregated, „Global Model“ and sends such Global Model back to the clients. The clients then use this Global Model to train it with their own Client Data, and the process begins again.

The below data flow graphic distinguishes between the different roles: Client is collecting Client Data (1) and is training with such Client Data, either on its own (2a) or with XAIN as its processor (2b). XAIN is aggregating all Local Models to one Global Model (3) and Client is using the Local Model for its own prediction purposes (4).

Since the quality of the Client Model is decisive for the quality of the prediction and decisions made by Client on the basis of the Client Model, every Client has an interest in aggregating the Global Model with its Client Model to get better results. Since the Global Model is dependent on Clients providing their Local Models, and, because of this, since every Client is committing to the Global Model, the entire procedure is called Federated Machine Learning.

The scope of this paper is to outline how Client Data is anonymized during FedML.

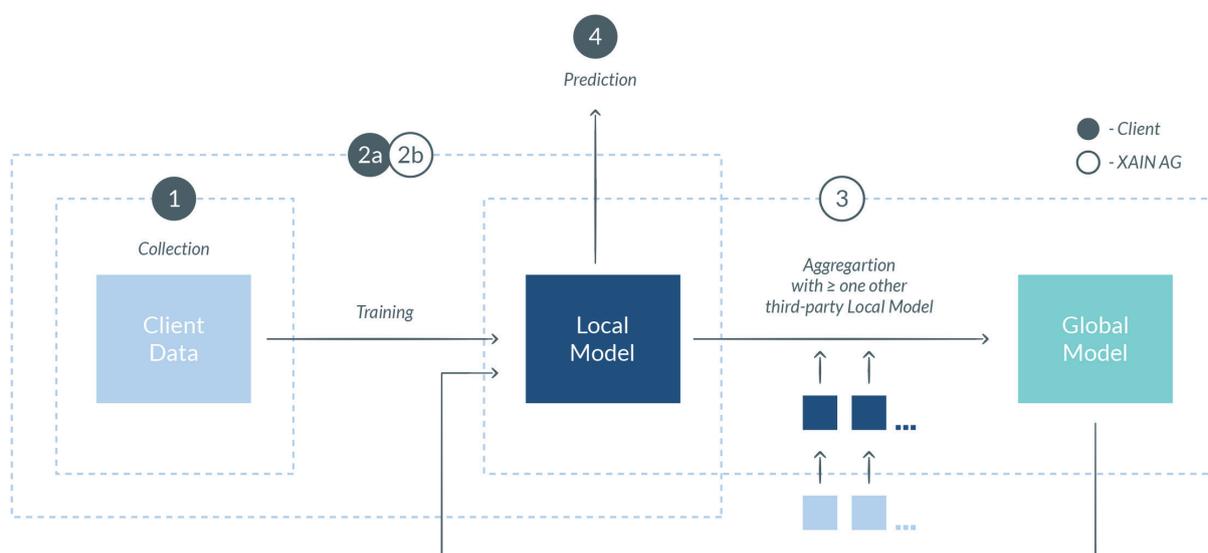


Figure 1: Data Flow in Federated Machine Learning scenarios

## B. Requirements for privacy

„Personal Data“ is, according to Art. 4 (1) GDPR, any information relating to an identified or identifiable natural person. Data, which is solely related to machines or companies, for example, is not considered Personal Data in terms of the GDPR but may of course nevertheless be subject to confidentiality obligations or qualified as trade secrets.

### I. PERSONAL DATA

In a GDPR context, data is anonymous and therefore not Personal Data if modified in such a way that data subjects can no longer be identified. According to recital 26 of the GDPR, to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. Further, to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments (see recital 26 GDPR).

This means that no absolute anonymity is required for data to be considered anonymous. When assessing the likelihood of so-called re-identification attacks, one should not only consider the effort necessary for completing such re-identification attacks, but also the criticality and sensitivity of the data targeted by the attacks.

**Example:** Since XAIN together with its Clients strives to remove sensitive/critical data at the beginning of the process (see below, C.I ), one may assume that the likelihood for a third-party to attack such model is much lower, given the amount of time and effort necessary for any viable attack. This means that the threshold for data to be considered anonymous is also lower.

### II. TRADE SECRETS

As regards trade secrets, one may consider Art. 2 (1) lit. c) Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure: Trade secrets must be subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

### III. CONTRACTUAL CONFIDENTIALITY OBLIGATIONS

In confidentiality obligations and non-disclosure agreements, one usually finds a wording similar to „appropriate precautions“, „adequate means“, „keep confidential“ or „duties of a prudent businessman“. Those wordings typically shall not ensure an absolute confidentiality (which is practically impossible, at least as soon as human beings are involved) but use undefined legal terms (*unbestimmte Rechtsbegriffe*) which are subject to an interpretation according to the individual case.

### IV. SUMMARY

In essence, the aforementioned legal obligations are united by the obligation to apply „reasonable“ means which certainly have to consider the concrete circumstances.

## C. Privacy behind FedML

Federated Machine Learning consists of several techniques which aim at ensuring that Client Data is not made accessible to third parties, including other Clients of XAIN. In the following, we describe techniques which are used in FedML scenarios to „anonymize“ Client Data. We are convinced that some of those are already sufficient so that inferences about individual Client Data are reasonably not possible anymore, and this must apply even more so if all techniques are applied cumulatively, which is the case with FedML provided by XAIN.

## I. COLLECTION OF CLIENT DATA

As one of the first steps, XAIN together with its Clients strives to limit the amount of Client Data that is processed in a FedML algorithm to those which are strictly necessary for the Machine Learning to function. During such process, much Personal Data is typically removed because data such as names or social security numbers are, due to their randomness, usually not suitable for Machine Learning models - which seek to identify patterns.

**Example:** *If a model shall be created which allows predictions about the number of staff being ill at a certain point in time during the year, then the names of the employees are not necessary to train such a model.*

## II. TRAINING

As regards the remaining data which is used as Client Data, one has to bear in mind that such data is not stored in a Client Model in plain form, but, since it is model data after having been trained, by means of a parameter vector (see above, A, for an example). This parameter vector does not directly provide any information about the data which has been the basis for the training.

**Example:** *If the Machine Learning algorithm based on the Local Model is, put simply,  $y = 1.45x_1 + 5.34x_2$ , then there is no direct possibility to calculate from the value of  $y$  and the learned constants 1.45 and 5.34 part of the Client Data which has been used to learn that model.*

## III. AGGREGATION TO LOCAL MODEL AND GLOBAL MODEL

Aggregation is an anonymization technique. The more data is used for aggregation, the more secure it becomes. XAIN's FedML algorithms usually uses at least three Clients.

**Example:** *Since the age of three persons with 32, 34 and 38 years is aggregated to 34.67, this data cannot be used to single-out an individual from the Source Data.*

There are two aggregations taking place:

- ▶ First, during the training, the trained data is aggregated with the Global Model from the previous iteration to get the Local Model as an outcome.
- ▶ Second, all Local Models are aggregated to get the Global Model.

In the first step, each Client uses only their own Client Data directly. In the second step, no Client Data at all is being used directly.

## IV. CONTRACTUAL SAFEGUARDS

Apart from the more technical safeguards described above, XAIN has and will put in place various legal and factual measures to further minimize risks in the extremely unlikely event that a person could make relevant inferences from model data about individuals.

Those measures include:

- ▶ XAIN concludes agreements with its Clients which shall ensure the confidentiality of the models and which shall forbid Clients to access the models other than with XAIN's software, which means that, legally, Clients are not allowed to make any attacks on the models.
- ▶ If the Client Data is critical or sensitive, XAIN will not pass the models to third parties which are not contractually bound, and XAIN will not make the models public, in order to minimize the number of persons having access to the models.
- ▶ XAIN will not unreasonably provide other Clients or third parties with the information on which Clients that have contributed to the models, nor in which way they have done that.

**Example:** *Even in the extremely unlikely scenario that an attacker could get the information that the number of staff being ill in a company at a certain point in time is 50 %, then the attacker would still not know to which company this single data applies.*



D.  
Summary

The models used in XAIN's FedML Platform are, in our view, anonymous in the sense of the law, as outlined above.

**PLEASE NOTE:**

Our intention with this paper is to inform the public about privacy techniques applied in Federated Machine Learning services provided by XAIN AG. This paper pursues a general approach, does not consider any individual Client case, reflects our personal legal view on FedML and is certainly not to be considered as legal advice. Nothing in this document shall be construed as a warranty of any kind. If you have any questions regarding Federated Machine Learning services provided by XAIN AG, please write us an e-mail: [info@xain.io](mailto:info@xain.io).

