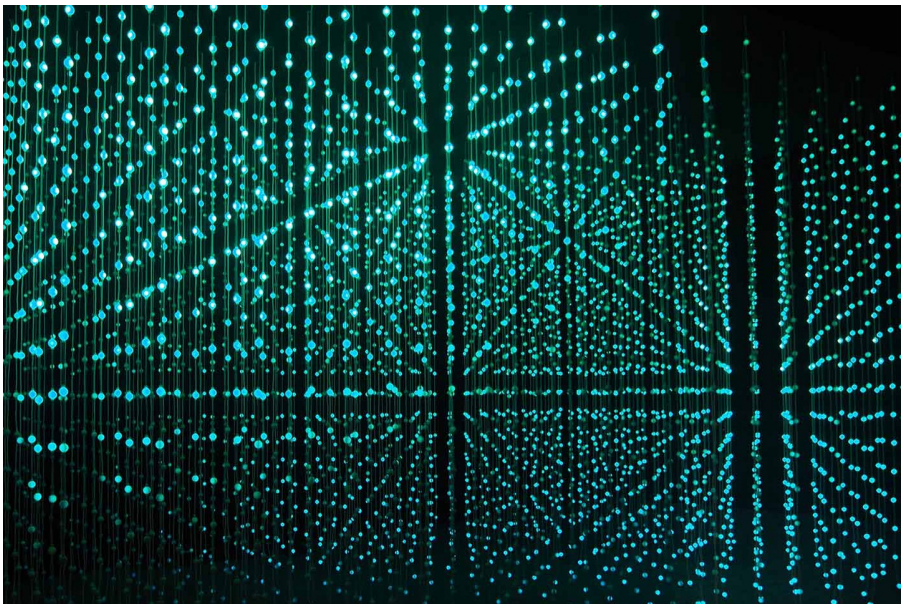
DATA SCIENCE

How will the GDPR impact machine learning?

Answers to the three most commonly asked questions about maintaining GDPR-compliant machine learning programs.

By Andrew Burt. May 16, 2018



Light structure (source: Pixabay)

Check out Steve Touw's session "How will the GDPR impact machine learning?" at the Strata Data Conference in London, May 21-24, 2018.

Much has been made about the potential impact of the EU's General Data Protection Regulation (GDPR) on data science programs. But there's perhaps no more important—or uncertain—question than how the regulation will impact machine learning (ML), in

particular. Given the recent advancements in ML, and given increasing investments in the field by global organizations, ML is fast becoming the future of enterprise data science.

This article aims to demystify this intersection between ML and the GDPR, focusing on the three biggest questions I've received at Immuta about maintaining GDPR-compliant data science and R&D programs. Granted, with an enforcement data of May 25, the GDPR has yet to come into full effect, and a good deal of what we do know about how it will be enforced is either vague or evolving (or both!). But key questions and key challenges have already started to emerge.

1. Does the GDPR prohibit machine learning?

The short answer to this question is that, in practice, ML will *not* be prohibited in the EU after the GDPR goes into effect. It will, however, involve a significant compliance burden, which I'll address shortly.

Technically, and misleadingly, however, the answer to this question actually *appears* to be yes, at least at first blush. The GDPR, as a matter of law, does contain a blanket

prohibition on the use of automated decision-making, so long as that decision-making occurs without human intervention and produces significant effects on data subjects. Importantly, the GDPR itself applies to all uses of EU data that could potentially identify a data subject—which, in any data science program using large volumes of data, means that the GDPR will apply to almost all activities (as study after study has illustrated the ability to identify individuals given enough data).

When the GDPR uses the term "automated decision-making," the regulation is referring to any model that makes a decision without a human being involved in the decision directly. This could include anything from the automated "profiling" of a data subject, like bucketing them into specific groups such as "potential customer" or "40-50 year old males," to determining whether a loan applicant is directly eligible for a loan.

As a result, one of the first major distinctions the GDPR makes about ML models is whether they are being deployed autonomously, without a human directly in the decision-making loop. If the answer is yes—as, in practice, will be the case in a huge number of ML models—then that use is likely prohibited by default. The Working Party 29, an official EU group involved in drafting and interpreting the GDPR, has said as much, despite the objections of many lawyers and data scientists (including yours truly).

So why is interpreting the GDPR as placing a ban on ML so misleading?

Because there are significant exceptions to the prohibition on the autonomous use of ML—meaning that "prohibition" is way too strong of a word. Once the GDPR goes into effect, data scientists should expect most applications of ML to be achievable—just with a compliance burden they won't be able to ignore.

Now, a bit more detail on the exceptions to the prohibition.

The regulation identifies three areas where the use of autonomous decisions is legal: where the processing is necessary for contractual reasons, where it's separately authorized by another law, or when the data subject has explicitly consented.

In practice, it's that last basis—when a data subject has explicitly allowed their data to be used by a model—that's likely to be a common way around this prohibition. Managing user consent is not easy. Users can consent to many different types of data processing, and they can also withdraw that consent at anytime, meaning that consent management needs to be granular (allowing many different forms of consent), dynamic (allowing

consent to be withdrawn), and user friendly enough that data subjects are actually empowered to understand how their data is being used and to assert control over that use.

So, does the GDPR *really* prohibit the use of ML models? Not completely - but it will, in many of ML's most powerful use cases, make the deployment and management of these models and their input data increasingly difficult.

2. Is there a "right to explainability" from ML?

This is one of the most common questions I receive about the GDPR, so much so that I wrote an entire article devoted to the subject last year. This question arises from the text of the GDPR itself, which has created a significant amount of confusion. And the stakes for this question are incredibly high. The existence of a potential right to explainability could have huge consequences for enterprise data science, as much of the predictive power of ML models lies in complexity that's difficult, if not impossible, to explain.

Let's start with the text.

In Articles 13-15 of the regulation, the GDPR states repeatedly that data subjects have a right to "meaningful information about the logic involved" and to "the significance and the envisaged consequences" of automated decision-making. Then, in Article 22 of the regulation, the GDPR states that data subjects have the right not to be subject to such decisions when they'd have the type of impact described above. Lastly, Recital 71, which is part of a non-binding commentary included in the regulation, states that data subjects are entitled to an explanation of automated decisions *after* they are made, in addition to being able to challenge those decisions. Taken together, these three provisions create a host of new and complex obligations between data subjects and the models processing their data, suggesting a pretty strong right to explainability.

While it is possible, in theory, that EU regulators could interpret these provisions in the most stringent way—and assert that some of the most powerful uses of ML will require a *full* explanation of the model's innerworkings—this outcome seems implausible.

What's more likely is that EU regulators will read these provisions as suggesting that when ML is used to make decisions without human intervention, and when those decisions significantly impact data subjects, those individuals are entitled to some basic form of information about what is occurring. What the GDPR calls "meaningful information" and "envisaged consequences" will likely be read within this context. EU regulators are likely to focus on a data subject's ability to make informed decisions about the use of their data—basically, the level of transparency available to the data subject—based on information about the model and the context within which it's deployed.

3. Do data subjects have the ability to demand that models be retrained without their data?

This is perhaps one of the most difficult questions to answer about the impact of GDPR on ML. Put another way: if a data scientist uses a data subject's data to train a model, and then deploys that model against new data, does the data subject have any right over the model that their data helped to originally train?

As best as I can tell, the answer is going to be no, at least in practice—with a very theoretical exception. To understand why, I'll start with the exception.

Under the GDPR, all uses of data require a legal basis in processing, and Article 6 of the regulation sets forth six corresponding bases. The two most important are likely to be the "legitimate interest" basis (where the interests of the organization justify specific uses of that data, which might cover a use like fraud prevention) and where the user has explicitly consented to the use of that data. When the legal basis for the processing is the latter, the data subject will retain a significant degree of control over that data, meaning they can withdraw consent at any time and the legal basis for processing that data will no longer remain.

So, if an organization collects data from a data subject, the user consents to have their data used to train a particular model, and then the data subject later withdraws that consent, when could the user force the model to be retrained on new data?

The answer is only if that model *continued* to use that users' data. As the Working Party 29 has specified, even after consent is withdrawn, all processing that occurred before the withdrawal remains legal. So, if the data was legally used to create a model or a prediction, whatever that data gave rise to may be retained. In practice, once a model is created with a set of training data, that training data can be deleted or modified without affecting the model.

Technically, however, some research suggests that models may retain information about the training data in ways that could allow the discovery of the original data even after training data has been deleted, as researchers Nicolas Papernot and others have written about extensively. This means that in some circumstances, deleting the training data without retraining the model is no guarantee that the training data could not be

rediscovered, or no guarantee that the original data isn't, at least in some senses, still being used.

But how likely is training data going to be rediscovered through a model? Pretty unlikely.

To my knowledge, rediscovery of this sort has only been conducted in academic environments that are pretty far removed from the everyday realities of enterprise data science. It's for this reason that I don't expect models to be subject to constant demands of being retrained on new data due to the GDPR. Though this is *theoretically* a possibility, it seems to be an edge case that regulators and data scientists will only have to address if this specific type of instance becomes more realistic.

All that said, there's a huge amount of nuance to all these questions—and future nuances will surely arise. With 99 Articles and 173 Recitals, the GDPR is long, complex, and likely to get more complex over time as its many provisions are enforced.

At this point, however, at least one thing is clear: thanks to the GDPR, lawyers and privacy engineers are going to be a central component of large-scale data science programs in the future.

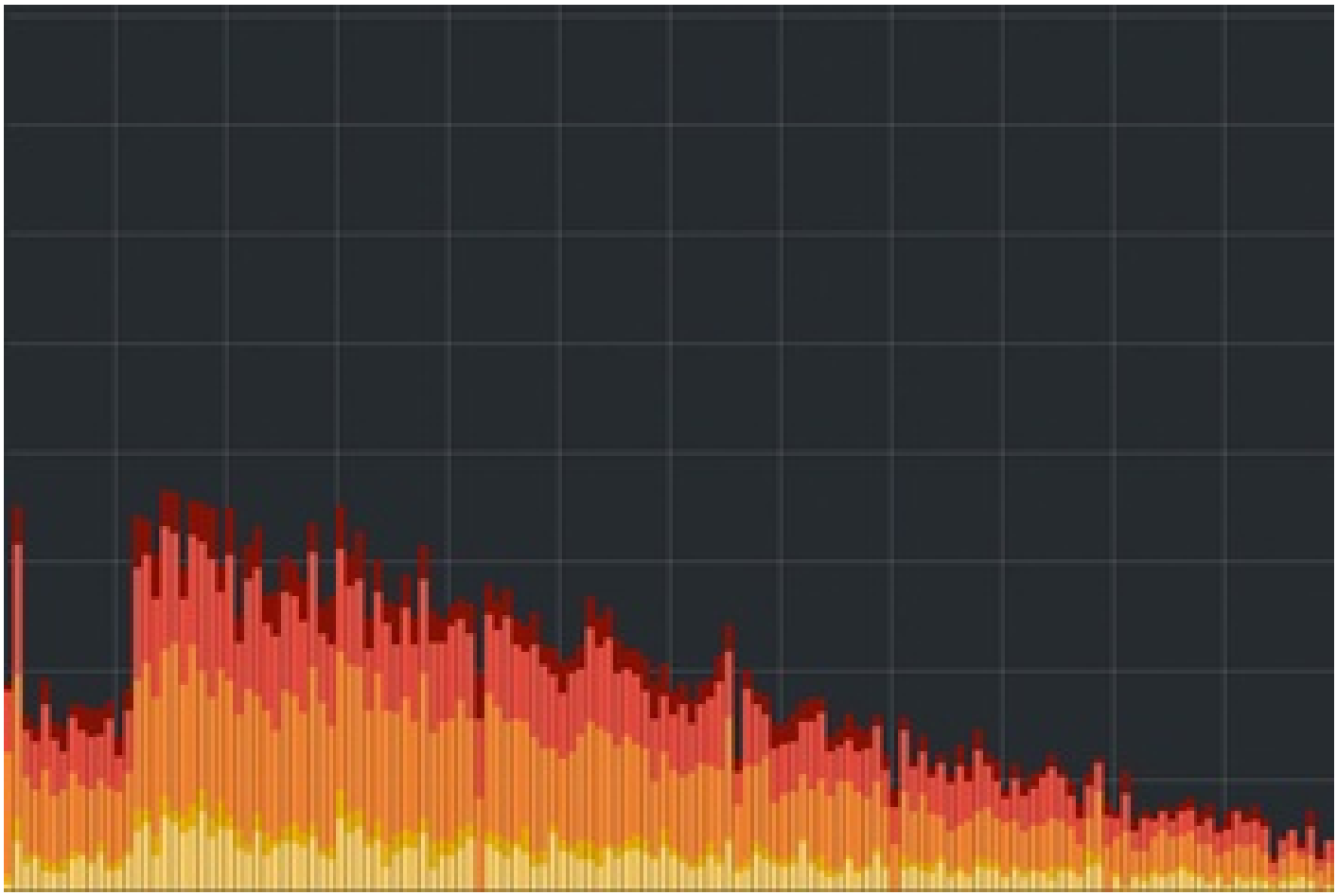
Article image: Light structure (source: Pixabay).

Andrew Burt

Andrew Burt is chief privacy officer and legal engineer at Immuta, a leading data management platform for data science.

more

DATA SCIENCE



Revealing the Uncommonly Common with Elasticsearch

By Mark Harwood

This webcast looks at how Elasticsearch is taking search engine technology and branching it out to provide insightful analysis of large datasets.

DATA SCIENCE

How intelligent data platforms are powering smart cities

By Ben Lorica

Smart cities and smart nations run on data.

DATA SCIENCE

Beyond algorithms: Optimizing the search experience

By Daniel Tunkelang

Making search smarter through better human-computer interaction.

DATA SCIENCE

Introducing Pandas Objects

By Jake VanderPlas

Python Data Science Handbook: Early Release