

# Establishing Guardrails for Using Customer Data in AI Training - A Blog Post by Michael Whitener & Christelle Pride

*This is the third in a series of VLP Technology Transactions Group articles on the legal challenges of artificial intelligence (AI).*

Previous blog posts in this series discussed the importance of your organization having a written AI usage policy and the necessary elements of such a policy. This blog post shifts the focus to your customer data: what safeguards are needed when using customer data for training your AI models?

Data is AI's lifeblood, fueling the development of increasingly sophisticated AI models. For data used to train AI models and their algorithms, quality is paramount: garbage in, garbage out. And what better source of quality data to enhance your AI tools than the data provided by your own customers? The "promise" is a virtuous circle whereby you harness the collective data of your customers to power AI-enhanced services and thus deliver far more value, and more efficiently, to each customer.

But here's the rub: customers tend to be squeamish about how their proprietary (and perhaps personal) data will be used by a service provider, other than as strictly necessary to provide services to the customer. At the same time, there is an expanding field of legal requirements that may govern how customer data can be used for AI purposes.

Below, we provide guidance on navigating the landscape of contractual and legal restrictions when using customer data for AI training purposes.

## 1. **Contractual Compliance**

From a contractual perspective, the first principle is that you can only use customer data within the scope permitted by your agreements with your customers. For purposes of transparency, and to maintain customer trust, any intended use of customer data for AI model training purposes should be fully disclosed in the agreed contract terms or linked policy documents. It's quite possible to satisfy this transparency obligation while at the same time assuring your customers of the benefits to be reaped from allowing this use of customer data.

Contract language covering use of customer data for AI training ideally should include the following elements:

1. *Informed consent.* Obtain explicit, informed consent from customers for the intended uses of their data in AI training. This means clearly explaining how the data will be utilized and the purposes of the AI training.

2. *Data usage limitations.* Commit to limitations on using customer data for AI training, including a commitment not to sell or share customer data with third parties without customer consent.
3. *Anonymization/de-identification.* Agree to anonymize or otherwise de-identify customer data, such that the data cannot be used to identify any individual or the customer itself. If personal information can be excluded from training data without limiting the AI model's functionality, all the better.
4. *Data security.* Provide assurances about security measures such as encryption in place to protect customer data from unauthorized access, misuse or breaches.
5. *Data minimization.* Agree to only use customer data that is reasonably necessary for AI training purposes rather than taking a firehose approach to data ingestion.
6. *Compliance with data protection laws.* Agree to comply with data protection laws applicable to use of customer data, and consider indemnifying your customers for any breach of those applicable laws (perhaps subject to a liability cap).
7. *Data deletion.* Commit to deleting customer data once it's no longer needed for AI training (or other appropriate) purposes, or upon termination of the contractual relationship, whichever occurs first.
8. *Opt-out rights.* Although not always feasible, consider granting customers the right to have certain (if not all) of their data excluded from AI training data sets.

For your own protection, and to provide your customers with further comfort should they request verification, you should implement internal policies and procedures to ensure your compliance with these contractual protections.

A company intending to use customer data for AI training should also take the opportunity to explain the advantages for the customer, so the customer's upside is apparent. Depending on your business model, customer benefits may include (i) quality and efficiency improvements, (ii) more innovative features and products, (iii) predictive assistance based on analyzing trends and patterns in customer usage data, and (iv) services that are more specifically tailored to each customer's needs.

The flipside of providing transparency to and obtaining consent from customers is ensuring that your customers have all the requisite rights to allow your company to use their data as agreed. To that end, the contract terms should make your customers solely responsible for (i) data quality and accuracy and (ii) providing any notices and obtaining any consents and/or licenses (including IP licenses) necessary for your use of their data.

AI model training is an iterative process, enabling the model's performance to improve as it learns from prior feedback and results. IP law hasn't yet definitively addressed whether a customer whose data is used to train an AI system may have a claim to the model itself. To address this uncertainty, service provider contracts should include language stating that: (i) the service provider owns all IP rights to the improved AI model; and (ii) the improved AI model is not considered part of the customer's confidential information.

## 2. Legal Compliance

Although AI regulation is still in its infancy, there are both current and pending laws that may impact your use of customer data for AI training.

In the U.S., the Federal Trade Commission has broad authority to prevent “unfair or deceptive” trade practices. The FTC has already begun exercising that authority in the AI arena, including issuing a **preemptive warning** that “quietly changing your terms of service” to permit using customer data to fuel AI products could violate the FTC Act.

A powerful tool in the FTC’s arsenal is “algorithmic disgorgement”: enforced deletion of algorithms developed using impermissibly collected data. The FTC has already used that tool in several enforcement actions – most recently against Rite Aid last December.

While a federal AI law isn’t even on the horizon, in October 2022, the White House released a non-binding Blueprint for an AI Bill of Rights that includes “notice and explanation” as one of its five principles. Meanwhile, a number of states have enacted or proposed laws to regulate AI, and recent state privacy laws such as the CCPA address automated decision-making and profiling.

In the EU and the UK, the GDPR and its UK equivalent already give data subjects broad rights regarding their personal data, including rights of access, correction and deletion. How would that work if your customer wants you to delete any personal data associated with an individual from your AI training data set? In current AI models, it’s not feasible to remove data from the AI system and have the AI algorithms persist with their original training. If eliminating all personal information from your training data isn’t practical, consider privacy-enhancing or privacy-enabling technologies such as differential privacy to anonymize or at least pseudonymize training data.

The newly approved EU AI Act is a game-changer: the first comprehensive legal framework to regulate the use and deployment of AI systems, with extraterritorial reach. The transparency and accountability requirements may directly impact your use of customer data for AI training, including obligations to produce summaries of data used for training models, depending on the Act’s risk classification of the AI model.

It’s not yet clear whether the EU AI Act will become the global benchmark for AI regulation, as the GDPR has for privacy rights. But already the UK, Canada and Brazil, among other countries, are following in the EU AI Act’s footsteps and considering risk-based AI laws.

Even in the absence of applicable AI regulations, there is general agreement on the characteristics of “trustworthy AI,” including: human-centric, accountable, transparent, explainable, fair and nondiscriminatory (free from bias). These characteristics should be kept top of mind when training AI models on customer data.

### **3. Final Thoughts**

Companies that prioritize privacy, transparency and robust governance in their use of customer data for AI will be best positioned for long-term success. Those that fail to do so risk regulatory enforcement, reputational damage, and erosion of the customer relationships they seek to enhance through AI.

Your use of customer data for AI training can be a powerful driver of innovation, benefiting you and your customers alike. By establishing clear contract terms and rigorously complying with legal obligations, you can harness the full potential of AI while respecting your customers’ rights and earning your customers’ trust.