Data Anonymization: Not as Simple as It Seems

October 21, 2025

Authors

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Ghiles Helli

Lawyer

Blind spots to watch for when anonymizing data

Anonymization has become a crucial step in unlocking the value of data for innovation, particularly in artificial intelligence. But without a properly executed anonymization process, organizations risk financial penalties, legal action and serious reputational harm, with potentially significant consequences for their operations.

Understanding the anonymization process

What the law says

Under Quebec's *Act respecting the protection of personal information in the private sector* (the "**Private Sector Act**") and the *Act respecting Access to documents held by public bodies and the Protection of personal information* (the "**Access Act**"), information concerning a natural person is considered anonymized if it irreversibly no longer allows the person to be identified directly or indirectly. Since anonymized information no longer qualifies as personal information, this distinction is of crucial importance. However, beyond this definition, neither Act provides details on how anonymization should actually be performed.

To fill this gap, the government adopted the *Regulation respecting the anonymization of personal information* (the "**Regulation**"), which sets out the criteria and framework for anonymization, grounded in high standards of privacy protection.

What organizations need to know before starting

Under the Regulation, before beginning any anonymization process, organizations must clearly define the “serious and legitimate purposes” for which the data will be used. These purposes must comply with either the Private Sector Act or the Access Act, as applicable, and any new purpose must meet the same requirement.

The process must also be supervised by a qualified professional with the expertise to select and apply appropriate anonymization techniques. This supervision ensures both the proper implementation of the chosen methods and the ongoing validation of technological choices and security measures.

The four key steps of data anonymization

1. **Depersonalization**

   The first step is to remove or replace all personal identifiers, such as names, addresses and phone numbers, with pseudonyms. It is essential to anticipate how different data sets might interact, in order to minimize the risk of re-identifying individuals through cross-referencing.

2. **Preliminary risk assessment**

   Next comes a preliminary analysis of re-identification risks. This step relies on three main criteria: individualization (inability to isolate a person within a dataset), correlation (inability to connect datasets concerning the same person) and inference (inability to infer personal information from other available information). Common anonymization techniques include aggregation, deletion, generalization and data perturbation. Organizations should also apply strong protective measures, such as advanced encryption and restrictive access controls, to minimize the likelihood of re-identification.

3. **In-depth risk analysis**

   After the preliminary phase, a deeper risk analysis must be conducted. While no anonymization process can eliminate all risk, that risk must be reduced to the lowest possible level, taking into account factors such as data sensitivity, the availability of public datasets and the effort required to attempt re-identification. To sustain this low level of risk, organizations should perform periodic reassessments that account for technological advances that could make re-identification easier over time.

4. **Documentation and record-keeping**

   Finally, organizations must keep a detailed record describing the anonymized information, its intended purposes, the techniques and security measures used, and the dates of any analyses or updates. This documentation strengthens transparency and demonstrates that the organization has fulfilled its legal obligations regarding anonymization.