

CONTRACTS

Legal Landscape for Agri-Food Data

Canadian Agri-Food Data Initiative
April 2024

CADI-Legal-2024-01

Authors

David Fewer, Director and General Counsel, [Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic](#), University of Ottawa

Kaitlyn Margison, J.D. (2023), [University of Ottawa](#)

Jordan Geist, J.D. (exp. 2024), [University of Ottawa](#)

We would also like to recognize the contribution of members of the Legal Landscape project working group including Natalie Kallio ([Canadian Centre for the Study of Co-operatives \(CCSC\)](#)), University of Saskatchewan (USask), Marc-André Pigeon (CCSC, USask), Bill Oemichen (CCSC, USask/University of Wisconsin), Anthony Rosborough (European University Institute/Dalhousie University), Josh MacFadden (Farm Credit Canada), Kristal Allen (Dentons), Tom Ogaranko (Octoco Inc.), Katie Szilagyi (University of Manitoba) and Jennifer Jannuska (Protein Industries Canada).

Editors

Dan Lussier, EMILI

Alicia Demanuele, EMILI

[EMILI](#) is an industry-led non-profit committed to accelerating Canada's growth as a leader in digital agriculture by supporting projects that advance innovative technologies and increase skills and training opportunities in the agri-food sector. Based in Manitoba, EMILI works with producers, industry and academia on projects across Canada to advance the adoption of innovative technologies and provide people with the skills and training required to succeed in the digital economy.

E M I L I

Canadian Agri-Food Data Initiative

The [Canadian Agri-Food Data Initiative](#) is working to build the data governance capacity of the Canadian agri-food sector through a unique combination of applied research projects and the development of data literacy training programs. The Data Initiative aims to empower farmers and other end-users of digital agriculture technology so they can make good decisions about their data and investments in digital tools.

Acknowledgements

EMILI would like to recognize the co-investment made by [Protein Industries Canada](#) through its Capacity Building Program that funded this project



About the Legal Landscape Series

Questions about contracts, ownership and privacy are among the first raised in any discussion about agricultural data. It is with that in mind that we created this series of guidebooks to address the key legal issues connected to data in agriculture and digital agriculture tools.

The intended audience for this series of guidebooks is broad, including farmers, technologists from digital agriculture technology (agtech) companies, agronomists, and stakeholders. We are aiming to reach non-lawyers working in the agri-food sector who have an interest in better understanding how the law impacts use of agriculture data. As a result, we have tried to keep the text as free as possible from legal jargon while maintaining the accuracy and integrity of the content.

This guidebook is the first in our Legal Landscape series that will, in turn, address other key topics such as data ownership and privacy.

Please note this document is not legal advice. Please seek out formal legal advice from an accredited legal professional if you have further questions related to your work with agri-food data.

How to Cite this Document

Fewer, Margison and Geist. *Contracts: Legal Landscape for Agri-Food Data*. EMILI Canada. CADI-Legal-2024-01. April 2024.



Key Takeaways



Contracts in agtech spell out how companies can collect and use farm data.



There are different types of agreements, like user agreements that explain the rules for using a service and data agreements that detail how your data can be used or shared.



It's important to know what you're agreeing to, especially around who can access your farm data and what happens to it if you stop using the service.



Understanding contracts helps you know where your data goes and how it is used.

Introduction

Contracts are the main legal tool we use to conduct business. We use contracts to buy and sell goods and services. Contracts are also essential tools for managing business relationships. We use contracts to secure rights and assets, implement policies, allocate risk, and follow legal rules, such as privacy law.

In the agricultural sector, farmers and businesses along the agri-food value-chain routinely enter into contracts, whether in selling farm products, purchasing farm inputs, or purchasing crop insurance. Contracts for agricultural software or digital agriculture technology (agtech) are similar to other contracts in the agricultural sector, but will include terms specific to software and data issues.

Agtech contracts are often composed of a bundle of agreements that each address distinct aspects of the technology. One or more of these agreements will address data issues relating to how data is created, collected, used, shared, processed, transformed, stored and more. We will focus our attention on these data-related aspects of agtech contracts. For data originators, such as farmers, understanding these agreements is central to understanding how agtech companies use contracts to obtain rights over farmers' data and handle their agriculture data. This can be challenging due to the complexity of the various agreements and the dense legal language in some contract text.

This guidebook's first section addresses contract law: the principles of contracting, types of contracts, key terms and their interaction with legislation. This is followed by a section providing answers to common questions about agtech contracts. Note that we will use the terms agtech and digital agriculture interchangeably throughout the guidebook.



Legal Principles

Understanding the legal principles that govern contracts will help you to protect your interests when entering into agreements. This section covers the types of contracts found in digital agriculture, their key components and how they interact with legislation. This section aims to make this complex topic easier to understand, helping farmers and agribusinesses navigate their contracts more confidently.

A contract is a legally binding agreement between two or more parties, such as a company, co-operative, incorporated non-profit or individual. A party initiates a contract by extending an offer laying out specific terms and conditions. The contract comes into effect when the other party explicitly accepts the offer. Acceptance of a contract creates legal obligations between the parties.¹

Contracts are valuable because they are meant to make promises enforceable. We can have faith in our agreements because we can rely on the law to enforce those agreements that we put into contract. For this reason, parties (e.g. companies, producers) use contracts to facilitate the sale or supply of their products and services.

In digital agriculture technology, contracts play an additional role: to secure rights to collect, access and use farm data. Data contracts are necessary for agtech companies because they ensure consent is obtained to collect, use and process a farmer's agricultural and business data. But data contracts do more than simply securing data rights. Contracts outline the responsibilities of each party involved and allocate associated risk. Key questions typically addressed in data contracts include: How will the data be used? What kinds of data is involved? Who bears the risk of loss? and What kind of security can the parties expect to safeguard sensitive data?



Types of Contracts

Farmers and other end-users of digital agriculture technology will encounter several different types of contracts. This section describes the three most common types of agreements used in agtech applications: (a) user agreements, (b) data agreements and (c) confidentiality agreements.

Each type of agreement has a unique purpose. Therefore, it is common for a single purchase, or transaction, to include several types of agreements, each focused on slightly different elements of the overall contract (e.g. [Farmobile's equipment lease and data upload agreement](#)).

User Agreements

User agreements are legally binding contracts governing the use of a service or product. Common user agreements include: (1) end-user licence agreements (EULAs), (2) terms of service agreements (ToS), and (3) privacy agreements.

1. End-User Licence Agreements (EULAs)

An end-user license agreement (EULA) is a software agreement that gives a user the right to use a software application for a defined purpose and may include restrictions on what the user can do with the software.²

For example, [John Deere's License Agreement for embedded software](#) gives users the right to use the software while restricting them from reproducing, modifying or leasing the software or the data generated within the software.

2. Terms of Service (ToS)

A terms of service (ToS) agreement specifies the rules the consumer must follow in order to continue using the service. These rules may be detailed in other agreements bundled with the ToS including privacy policies, intellectual property notices, opt-out provisions and/or liability provisions.³

Examples include [Bayer Climate FieldView's Terms of Service](#) and [Valmont Industries' Terms of Service](#). Note that terms of service agreements may sometimes be called terms of use agreements.

3. Privacy Agreements

Privacy agreements are contracts used to obtain an individual's agreement to an organization's privacy practices. Privacy policies, or privacy notices, are not typically contracts on their own. Rather, they are legal documents that may be incorporated into the terms of a contract. Privacy notices describe the personal information (PI) an organization collects, the purposes for the PI collection and how the organization stores, shares and uses PI. See the section [How do Contracts Interact with Legislation?](#) for more information about rules that influence the content of privacy notices.

For an example of a privacy notice, see the [Farm Credit Canada Privacy Policy](#) which is incorporated into the [Ag Expert Software Terms of Service](#).

Data Agreements

Data agreements set out the terms and conditions for how technology companies can use, share or process data. Some agreements governing those activities include: (1) data use agreements, (2) data processing agreements, and (3) data licensing agreements. Keep in mind that data agreements with different names can be quite similar. It is always important to examine the substance of the agreement to understand what it means for your data.

1. Data Use Agreements (DUAs)

A data use agreement (DUA) specifies the terms under which a data collector, such as an agtech company, can use collected data.⁴ Agtech companies use DUAs to obtain permissions to collect data from a grower or other end-user. For example, a DUA may obtain permissions from a user to allow the company to analyze, share, or process their data. A DUA may also specify limitations on a company's ability to use collected data. For instance, a DUA can prohibit sharing collected data with third parties.

Examples of DUAs include the [Growmark Data Use Agreement](#), the [Farm Credit Canada Ag Expert Data Use Policy](#) and the [Telus Agriculture and Consumer Goods Data Use Policy](#), which also includes their privacy policy. The Agriculture Data Transparent organization also provides a [template data use agreement](#) that is simple and easy to read.

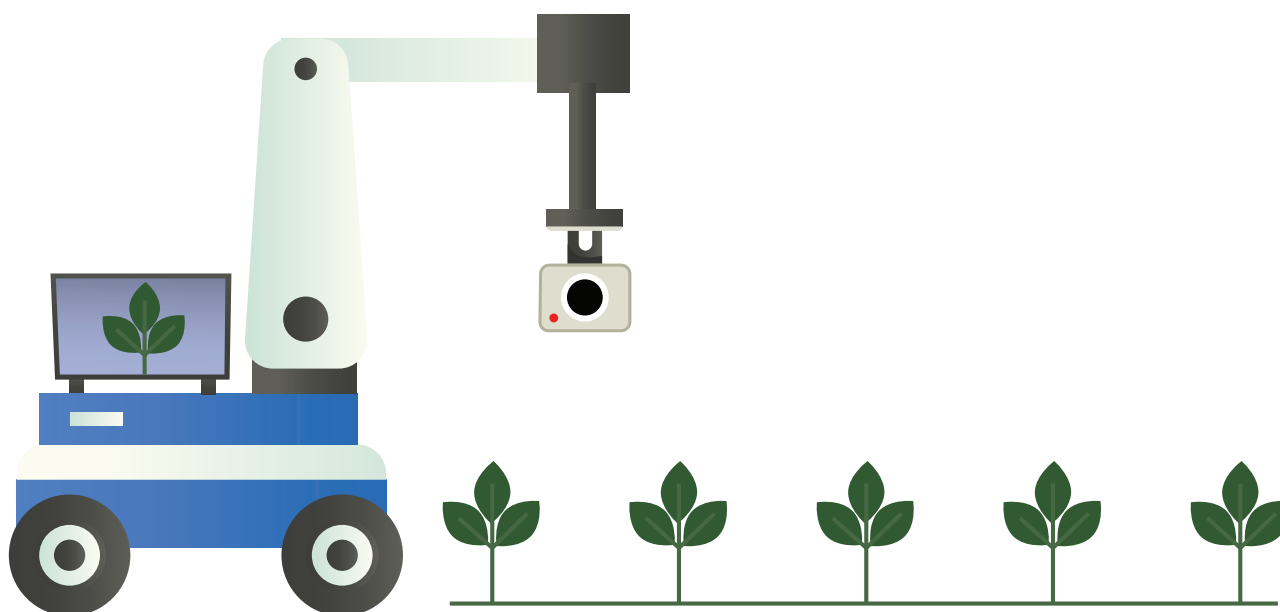
[Data sharing agreements](#) are a type of data use agreement. Where DUAs usually allow

data to flow from an end-user (e.g. farmer) to a technology company, data sharing agreements are used to accommodate data flowing in both directions between two or more organizations.⁵

2. Data Processing Agreements (DPAs)

A data processing agreement (DPA) is an agreement between two companies: one with data to be processed and one that offers data processing services.^{6,7} An agtech company will use a DPA when engaging a third party company to process or analyze data on their behalf. For example, companies can use services like [Google Analytics](#) to analyze information on how visitors use their website (e.g. time spent on different pages).

A DPA will detail requirements and obligations for processing, storing and protecting the data. The contract will also specify the rights of each party to both the original data being analyzed as well as any new data created under the processing contract.



3. Data Licenses

A data license specifies conditions a data source attaches to the use of their data by another person, or organization.⁸ A data license in this sense simply establishes legal conditions to use data. Data licenses can stand alone, imposed by the data originator, or data source, on anyone who may wish to use the data. While not truly contracts when used this way - since there is no bargain or exchange between the parties - courts will nonetheless enforce the terms of a license. These one-way legal documents can be very useful to efficiently grant access to data, and can even be made to be machine-readable so that data may be accessed using software via [APIs](#). There are numerous standard data licenses developed by independent organizations, such as [Creative Commons](#).

A contract built around a data license is known as a *license agreement*. In fact, data licenses are built into almost all data agreements as the part of the agreement that establishes the legal conditions for the use of the data. A data license agreement is similar to a data use agreement (DUA)—both govern how data is used. Data license agreements tend to be standardized and imposed by the data source, rather than a technology provider. In contrast, data use agreements tend to be customized by the organization that drafts and imposes the agreement. However, this is a generalization and in practice very similar agreements could be called a *license agreement* or a *data use agreement*.

[Telus' Data for Good program](#) offers an example of a data license agreement. [Telus' data license](#) grants access to de-identified data from Telus telecommunications systems for research and other socially beneficial purposes. Data provided by Telus under this data license is subject to standardized contractual restrictions, including limitations on the purpose of access, time period of use, sharing and retention of such data and a prohibition on attempts to re-identify the data.

Open Data Licenses

Open data providers want to encourage others to use, build upon, combine and innovate with their data. As a result, open data licenses are permissive licenses that have few—if any—restrictions on how data may be used. For example, the Government of Canada provides large amounts of information under an open license for use by businesses, individuals and non-profit organizations. Similar open data portals are also provided by other governments (e.g. City of Winnipeg).

Confidentiality and Non-Disclosure Agreements

Another type of agreement farmers and other agtech software users may encounter is a confidentiality or non-disclosure agreement – these terms are often used interchangeably. These agreements are often found within a bundle of agreements or as a clause within a larger contract. Confidentiality and non-disclosure agreements set terms and conditions for using information that is not publicly available.

These types of agreements are often used to protect sensitive information, including proprietary technologies and trade secrets such as business strategies or unique methodologies. Confidentiality and non-disclosure agreements are commonly used by technology companies, including agtech companies, as a method of protecting intellectual property and trade secrets during interactions with clients or other stakeholders.

Components of Contractual Agreements

As illustrated above, technology companies use contracts to obtain permissions to collect and use data and impose obligations or restrictions with respect to data. This section describes some commonly encountered components of data contracts: (a) scope, (b) consent, (c) third party and secondary use, (d) contract termination and (e) jurisdiction.

Scope

All contracts contain specific terms to define their scope—what is included and excluded from the agreement. In a data agreement, the scope outlines the kinds of data being collected, the activities, services, or products that are covered and how the technology company plans to use this data. These terms are often written in a broad manner to give technology companies the flexibility to adapt their services or products over time without needing to rewrite the contract.

It is not uncommon for the contract to exclude certain things from the scope of contract. For example, a contract might clearly state that it offers no warranties or limit the company's responsibility if something goes wrong.

Consent

Technology companies need explicit permission to use and share data. The contract itself usually seeks this permission, often referred to as consent. Consent clauses allow the company to use the data as outlined in the agreement.

Often, the consent sought in an agreement covers all anticipated dealings with the data, including internal use and any sharing of the data with third parties. It typically also covers all of the anticipated rights associated with the data including confidentiality and privacy rights in personal information.

In Canada, if a company wants to collect, use or share data that contains personal information, [Canadian privacy law](#) requires the company to actively obtain consent. In practice, this means having a user agree to sharing their personal information, often by checking a box in an online form.

Contracts of Adhesion - Take it or Leave it!

Many agtech and agriculture data contracts are contracts of adhesion, where the producer, or end-user, is not given the opportunity to negotiate terms and the allocation of risk. In this sense, adhesion contracts say "take it or leave it." The producer either accepts the standard terms and uses the product or service, or they reject the terms and cannot use the product or service. Contracts of adhesion are commonly encountered in many digital products and services across multiple industries (e.g. [WhatsApp Terms of Service](#)).

Third-Party Access and Secondary Use

Third-party access and secondary use are common contract terms that can allow a company to share your collected data or use it in an unfamiliar or new way.

Third-party access occurs when data is provided to another organization outside of the contract. For example, an agtech company may want to share producer data with a third-party data processor, such as a data analytics company. The data contract may also define the procedure by which a farmer, or user of the software tool, may ask for their data to be shared with a third party of their choice, such as an agronomist or another trusted advisor.

Secondary use is a contract term that allows data to be used beyond the specific reason for which the data was primarily collected. For example, health care data initially collected for diagnostic purposes may be subsequently used for clinical research.⁹ In the agricultural sector, an agtech company may collect agricultural data to provide precision agronomy services, but the company may also use the data for training artificial intelligence models or developing new products. The company may also need to share the data with a third party to perform a data analysis that informs how the application will work.

Depending on the third-party access and secondary use terms in the contract, the user may lose control, or the ability to make further informed decisions, over how their data is used and who is using it. However, secondary use and third-party access to data can also benefit the end-user. For example, an agtech company could use farm data it collected to create an artificial intelligence tool that improves the service it provides to farmers.

Contract Termination Deletion and Return of Data

What happens to your data when you stop using a service, software or piece of technology and the data agreement comes to an end? The details on how your data is handled at the end of the contract are important parts of the contract itself. Contract termination clauses differ between agreements as some require the data collector (e.g. agtech company) to delete the data after the contract's expiration, while others require the user to request data deletion. For example, see the *Your Ag Data at Termination* section in [Farm Credit Canada's AgExpert data use policy](#).

A contract with an agtech company often includes specific terms, referred to as data portability provisions, around how—or if—you can request your original data back from the company. Depending on the data portability provisions set out in the contract, companies may state that they will only return data to users in a proprietary format, making it more difficult or costly to use the data on another technology company's platform.

Agtech companies may handle the original farm data and aggregated data differently at the end of the contract. An aggregated dataset is a dataset created by grouping data gathered from different sources, or customers, together. In the context of contract termination, it is typically not possible for the technology company to remove an individual user's data from aggregated datasets. For example, in their [Terms and Conditions CarbonTerra](#), a Saskatchewan-based soil carbon startup, assigns ownership rights and control of the original entered data to the farmer but claims company ownership over aggregated datasets. As a result, even after contract termination, the user's contribution to aggregated data will remain with the company. In effect, by entering into the contract that assigned ownership of the aggregated data to the company the user does not have control over how the aggregated data is used, even after their original data is deleted.

Aggregated Data

Aggregated data is a collection of data made up of several data sources such as individuals, users, businesses or farms. Many contracts have terms outlining how individual data may be combined into an aggregated dataset and how companies can use the aggregated data.

Aggregated datasets can be used to analyze trends and correlations within the population of data contributors. For example, agtech companies can use aggregated data from many farm customers to provide benchmarking services and recommendations for seeding, nutrient or crop protection applications.¹⁰

An aggregated dataset may also be anonymized by removing specific data that identifies any single person, business, or contributor to the dataset (i.e. de-identification). That said, it is important to know that despite best efforts, the data de-identification process may not be perfect—in some cases it can be possible to re-identify individual data contributors from aggregated data.¹¹ As a result, it is important that technology companies have policies and practices in place to ensure the security of anonymized aggregated datasets.

Jurisdiction International Data Flows

Cross-border data flows are common within the agriculture sector as agtech companies work with domestic and international customers. In addition to carrying out business in multiple jurisdictions, many agtech companies move data between jurisdictions to provide services and access the personnel and infrastructure needed to support those services. For example, a data centre may be located in the US even though the agtech company has operations in Canada and is serving Canadian customers.

Cross-border data flows can create legal uncertainty as the laws governing data use may differ from one jurisdiction to the next. For example, a company may store and process data in California that was generated on a farm in British Columbia. In this case, depending on the contract terms, the farm data can be subject to the laws in California, as opposed to those in British Columbia. Many organizations address this issue by using a standard set of data protection clauses that are compliant with common global privacy requirements. Notably, regardless of the contract terms, foreign national security and law enforcement authorities may be able to access data stored in foreign jurisdictions.¹²



How do Contracts Interact with Legislation?

Legislation, or statutes, can influence the terms of contracts, requiring or implying some terms and eliminating others. Two examples relevant to the agriculture technology sector are farm equipment and privacy laws.

Farm Equipment Laws

Most provinces have special laws addressing farm equipment contracts. For example, Ontario's *Farm Implements Act* enforces a minimum one-year warranty, sets rules for how contracts can be ended between distributors and dealers and provides rules for solving disagreements. These laws apply to all Ontario farm machinery contracts, whether they are included explicitly in the contract or not. Other provinces have similar laws, such as the *Farm Implement Act* in Alberta, the *Farm Machinery Equipment Act* in Manitoba and Saskatchewan's *Farm Security Act* and *Agricultural Implements Act*. This legislation applies to equipment and hardware, rather than software.

Privacy Law

Privacy laws require explicit terms to describe and authorize how businesses handle personal information. For example, Canada's federal and provincial private sector privacy laws (Quebec, Alberta, British Columbia) require businesses to obtain consent before collecting, using or disclosing personal information.

Consumer protection laws may also be relevant to agriculture technology and data contracts. For example, in Ontario under the *Consumer Protection Act*, class action waivers in consumer contracts are unenforceable so consumers retain their rights to band together to address things like faulty equipment. Other provinces have similar laws.

Plain Language

Although contracts are common in farming and in our everyday lives, many are long and complex. This complexity costs time and money and often leads to uncertainty.¹³ Reports indicate that less than 10% of people read the full terms of service or license agreements for digital apps before clicking agree.¹⁴

In response to this challenge, the legal community is moving towards plain language contracts that aim to simplify contractual language so non-lawyers can easily understand the agreement without additional context or explanation.¹³

In some cases, laws require plain language in relevant contracts. For example, privacy laws, such as the federal private sector privacy law, [PIPEDA](#), generally require organizations to inform individuals in plain language about the collection, use and disclosure of personal information.

There are no similar plain language laws for other types of business or farm data. However, the [Ag Data Transparent](#) (ADT) organization helps provide plain language information about agtech and agriculture data contracts by asking agtech companies to describe their data management practices in plain language as part of their certification process. To be certified by ADT, an agtech company submits their answers to [eleven standardized questions](#) describing their approach to data. These responses are analyzed by the ADT legal team to ensure they are aligned with the company's data contract and then posted on the ADT website (eg. [Farmers Business Network ADT questionnaire responses](#)).

Thumbs up grain contract

In 2023, a [Saskatchewan judge ruled that a thumbs up emoji](#) was sufficient to demonstrate acceptance of a grain contract offered over text message. As a result, the farmer in question was required to pay more than \$82,000 for failure to deliver the promised flax seed. The case serves as a reminder that attention to detail is critical when handling all contracts.



Putting it into Practice

As a farmer, what if I want to negotiate or make changes to the default farm data contract? How can I get help from a lawyer with an agriculture technology contract?

Many agriculture data contracts are contracts by adhesion—take it or leave it. In these circumstances, there is no opportunity to negotiate with the terms of the agreement.

However, in more comprehensive agreements there may be an opportunity to make changes to the default contract. If you want to negotiate or make changes to a default data contract, you can reach out directly to the agtech company to discuss your concerns and proposed changes. A lawyer can also be helpful in reviewing, interpreting and negotiating terms on your behalf to make sure an agreement

meets your needs. To find a lawyer, you can go through online legal directories such as the [Canadian Bar Association](#) or contact your provincial or territorial bar directory.

How do I know I'm giving consent for a company to use my farm data?

Your consent is confirmed once you agree to the terms and conditions outlined in a data contract that includes a section seeking such consent. This can take the form of signing a document, either by using pen and paper or an electronic signature, or clicking an *Agree* button within a software tool.

It is important to read the contract carefully. A consent clause may not be expressed explicitly, rather it may be a component of a larger bundle of agreements. If terms are unclear, you can reach out to the company to ask for clarity or ask a lawyer to review the contract.

Is clicking *Agree* within an app or software tool to a user agreement, or data contract, the same as signing a paper contract?

Yes, clicking *Agree* within an app or software tool is just as legally binding as putting pen to paper. The terms and conditions presented in the app or software tool constitute an offer presented to a user, clicking *Agree* is acceptance of the offer.

It can be tempting to simply click *Agree* after rapidly scrolling through the terms of service for a new software tool, or online service. But it is important to read and review the contract terms because, except under [extreme circumstances](#), courts will hold you to the contract terms you signed, or clicked *Agree* to.



What does it mean to enforce a contract? What happens if I have a problem with one of my agriculture technology vendors?

Enforcing a contract is about making sure everyone sticks to the agreed terms. If there is a breach of contract, a first step worth considering is communicating with the agtech company to attempt to resolve the issue. Miscues between service providers and their customers do occur, and sometimes these can be resolved with timely communication.

If no resolution is possible, or if the issue is significant, you may need to consider seeking legal assistance to address any breaches. There may be legal solutions such as mediation, arbitration or joining class actions for more wide-spread breaches affecting many people. Legal enforcement of a contract can be both time-consuming and expensive.

Is there any way to prevent my farm data from being stored outside of Canada? How do I find out where my technology provider stores my data?

To find out how your agtech company stores data, check the company's terms of service or privacy policy or ask them directly about data storage locations. If you want your data stored domestically in Canada, ensure this is stated explicitly in the contract. Be aware, though, some processes involving your data might still occur elsewhere, especially if third parties are involved. For instance, the company may use a third party based in the United States, or elsewhere, to process payments. Some companies may lack the technological capacity to store your data in Canada.

Key Takeaways



Contracts in agtech spell out how companies can collect and use farm data.



There are different types of agreements, like user agreements that explain the rules for using a service and data agreements that detail how your data can be used or shared.



It's important to know what you're agreeing to, especially around who can access your farm data and what happens to it if you stop using the service.



Understanding contracts helps you know where your data goes and how it is used.

References



1. Mueller W. [CED Contracts](#). WestLaw. Accessed November 2022.
2. Rouse M. [What is an End-User License Agreement \(EULA\)? - Definition from Techopedia](#). Techopedia. 2022. Accessed November 2022.
3. Rouse M. [What are Terms of Service \(ToS\)?](#). Techopedia. 2022. Accessed November 2022.
4. [Data Use Agreements \(DUAs\)](#). University of Pittsburgh. 2022. Accessed November 2022.
5. [Guidance on Preparing Information Sharing Agreements Involving Personal Information](#). Government of Canada. 2010. Accessed November 2022.
6. Kovacsics P. [Everything you need to know about a Data Processing Agreement | Tresorit](#). Tresorit Blog. 2018. Accessed November 2022.
7. [The Ultimate Guide to Data Processing Agreements](#). Secure Privacy. 2022. Accessed November 2022.
8. [Data Licences](#). How to Fair. Accessed November 2022.
9. [Secondary Use of Data](#). Sunnybrook Research Institute. 2022. Accessed November 2022.
10. Fulton M, Pigeon MA, Oemichen B, Yang Y. [Digital Technologies and the Big Data Revolution in the Canadian Agricultural Sector: Opportunities, Challenges and Alternatives](#). Canadian Centre For The Study Of Co-Operatives. 2021. Accessed November 2022.
11. [Consumers Anonymous? The Privacy Risks of De-Identified and Aggregated Consumer Data](#). Office of the Privacy Commissioner of Canada. 2011. Accessed March 2023.
12. [Cross-border Data Flows: Security and Privacy Issues Within The EU and Beyond](#). Cyber Security for Europe. 2021. Accessed November 2022.
13. Burton S. [The Case for Plain-Language Contracts](#). Harvard Business Review. 2018 (January-February 2018):134.
14. LePan N. [Visualizing the Length of the Fine Print, for 14 Popular Apps](#). Visual Capitalist. Accessed November 2022.

EMILI

Accelerating Digital Agriculture



[EMILICanada.com](https://www.EMILICanada.com)



[@EMILICanada](https://www.linkedin.com/company/EMILICanada)



[@EMILICanada](https://www.x.com/EMILICanada)



info@EMILICanada.com

www.emilicanada.com