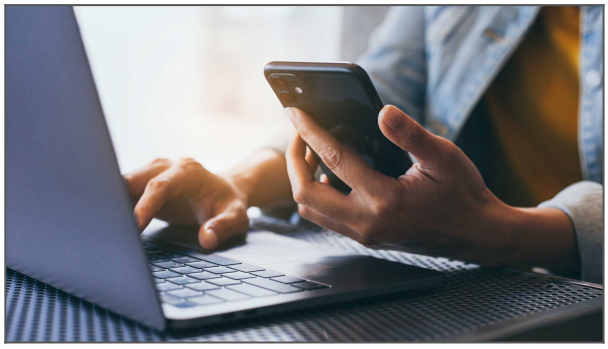
Terms of Use & Privacy Policy

Authors: Silvia de Sousa Kendall (Dell) Dyck

published 06/22/2021

The value of implementing Terms of Use and a Privacy Policy should not be underestimated.



How do Terms of Use Protect a Website Operator?

Terms of Use are crucial in protecting website operators (the "Operator") and informing users of a website (the "User") of the appropriate uses of a website. They are a legally-binding agreement between the Operator and the User. The User must agree to the Terms of Use in order to access the website and its services. A website's Terms of Use may require a User's active agreement by prompting a selection of either I ACCEPT or I DO NOT ACCEPT. Alternatively, a User's continued use of a website may also indicate understanding of and agreement with the Terms of Use. If a User does not agree with the Terms of Use, they are not permitted to access the website.

Terms of Use set out limitations of liability and establish ownership of intellectual property, such as content. Although the Operator aims to provide accurate and current information, Terms of Use can protect the Operator from liability against errors, misprints or omissions on the website. Terms of Use can state that the Operator is not responsible for the failure of encryption technology or the actions of third parties on their website, such as the distribution of a User's personal content by a third party. Further, Terms of Use can provide that the Operator is not liable for property damage, personal injury or monetary loss resulting from access and use of the website. Terms of Use can also have a governing law clause specifying that a dispute is to be resolved according to the laws of a certain jurisdiction.

Terms of Use can prevent abuses on behalf of the User by defining the allowed purposes for accessing and using the website, such as personal or commercial use. Terms of Use can state

that Users have an obligation to refrain from distributing unauthorized materials and cannot alter the website or transmit any malware or viruses. As part of the User's obligations under the Terms of Use, the User is responsible for checking the Terms of Use periodically as the Operator can change the terms without notifying the User. These changes are effective immediately and a User's continued use of the website signifies their agreement to be bound by these new terms. Moreover, the Operator holds discretion to terminate a User's access and use of the website.

Ultimately, Terms of Use provide Operators with ample protection but also inform the User of their responsibilities and restrictions when accessing and using a website. Such transparency is another step towards creating trust with the User.

What is a Website Privacy Policy?

A website privacy policy is a document on the website that describes how an organization collects, uses and discloses personal information, among other things. Personal information is defined under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") as information about an identifiable individual. Privacy policies include notice of certain practices, risks and individual rights as required by PIPEDA. While in and of itself, a website privacy policy is not a contract, it is often incorporated by reference into the Terms of Use (a unilateral contract) such that when the User consents to the Terms of Use, they are also consenting to the website privacy policy.

Why do I need a Privacy Policy on my Website?

PIPEDA utilizes a consent-based model, meaning organizations must obtain meaningful consent in order to collect, use and disclose the personal information of Users. Although PIPEDA does not explicitly require a website privacy policy, there are several reasons why some kind of electronic notice like a privacy policy is necessary.

First, PIPEDA requires *meaningful consent*. This means that Users must be able to understand to what they are consenting. Depending on the information collected, that consent can be express or implied. Knowledge and consent to the collection, use and disclosure of personal information is required before they can occur. If customers are given access to the information contained in a privacy policy at the time they utilize an organization's services or purchase their goods, consent can be implied in certain circumstances. A website privacy policy can assist in achieving that, though in certain circumstances "just-in-time" notices should be considered as well.

Organizations must make information regarding their privacy practices and policies readily available, and must emphasize four key aspects:

1. What personal information is being collected;
2. With whom it is being shared;

3. For what purposes it is being collected, used and disclosed; and
4. Any risks of harm or other consequences.

Organizations must disclose specific information such as to whom complaints can be directed, how individuals can gain access to the personal information held about them, and how that information is used, among other things. Individuals must be able to access this information without unreasonable effort.

Second, is the reality of our world. Many commercial transactions (which PIPEDA governs) now occur online, even more so in a post-pandemic world. This means a significant amount of the personal information an organization is collecting, is collected online. PIPEDA requires organizations to provide certain information at or before the time of collection, meaning this information needs to be provided online somehow. A website privacy policy is a convenient way of providing such information.

Even if you do not collect any personal information, it is a good idea to have a website privacy policy that emphasizes that fact. The collection of personal data is so ubiquitous today that if a customer sees a website without a privacy policy, rather than assuming the organization does not collect personal information, they may conclude the organization is simply not being transparent about their practices. Trust and reputation are difficult to build, and easy to lose, even where the loss is not justified. Users should not have to guess as to what are an organization's privacy practices.

Organizations operating outside of Canada need to be aware of data protection and privacy laws in the foreign jurisdictions where they operate. For example, the **California Consumer Privacy Act (CCPA)** in the U.S. and the **General Data Protection Regulation (GDPR)** in the E.U. As the exclusive **Lex Mundi** member law firm for Manitoba, Canada, TDS assists clients with data protection and privacy law advice in 100+ countries around the world.

TDS offers these services on a fixed fee basis, providing clients with cost certainty and budget predictability. Please **contact us** if you need assistance regarding your Terms of Use and Privacy Policy.

Thompson Dorfman Sweatman LLP (TDS), its affiliate companies or its clients. The authors make no guarantees regarding the accuracy or adequacy of the information contained herein or linked to via this article. The authors are not able to provide free legal advice. If you are seeking advice on specific matters, please contact Keith LaBossiere, CEO & Managing Partner at kdl@tdslaw.com, or 204.934.2587. Please be aware that any unsolicited information sent to the author(s) cannot be considered to be solicitor-client privileged.

While care is taken to ensure the accuracy for the purposes stated, before relying upon these articles, you should seek and be guided by legal advice based on your specific circumstances. We would be pleased to provide you with our assistance on any of the issues raised in these articles.

 |