



# Signing Contracts While Working Remotely: Use of Electronic Signatures During COVID-19 Pandemic

July 27, 2020

By Amanda Branch and Siobhan Doody

In recent years, electronic signatures have been increasing in popularity for several reasons. For example, some organizations find it easier to store digital copies of contracts and want to reduce paper waste and storage where possible. Recently, the use of electronic signatures has accelerated given that many people around the world are now working remotely from home without access to a printer, scanner or fax machine.

Certain laws require documents to be signed. But, even when there is no legal requirement for a document to be signed, signatures can help demonstrate a party's agreement to be bound by the terms of a document. Signatures may be physical or electronic.

This high level overview of the use of electronic signatures in Canada will not address all of the legal complexities of electronic signatures that reach beyond the scope of this article, but rather will highlight some key considerations for adapting to working with documents electronically when physical signatures are not feasible.

In Canada, electronic signatures are regulated at both the federal and provincial level and are generally found to have the same validity as physical signatures. For the most part, the federal and provincial legislation relating to electronic transactions and e-commerce is consistent. Most provinces and territories have largely modelled their e-commerce legislation on the [Uniform Electronic Commerce Act](#) (the "UECA") which is designed to implement the principles of the [UN Model Law on Electronic Signatures](#) in Canada (Quebec's e-commerce law follows many of the same principles but does not directly implement the UN Model Law).

## What is an electronic signature?

An "electronic signature" is typically given a broad definition in the provincial legislation. For example, Ontario's [Electronic Commerce Act](#) ("OECA") defines an electronic signature as "electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document".

While the federal privacy legislation, the [Personal Information Protection and Electronic Documents Act](#) ("PIPEDA") includes a definition of electronic signature and specific requirements for the use of such signatures, it is important to note that PIPEDA's provisions relating to the use of electronic signatures apply only to statutes listed in the applicable Schedules. Having said that, the requirements for electronic signatures as set out in PIPEDA can help guide best practices.

Electronic signatures are generally acceptable for contractual arrangements, including commercial agreements and some consumer contracts. It is important to note that the provincial legislation does not override the application of any other laws that prohibit or otherwise regulate the use of electronic signatures or electronic documents. Certain provincial legislation expressly prohibits electronic signatures from being used on specific documents. Further, certain provincial consumer protection legislation may have specific requirements for "internet agreements". For example, the Ontario [Consumer Protection Act](#) requires the supplier to provide the consumer with an express opportunity to accept or decline the agreement and to correct any errors before entering in to such agreement.

An electronic signature can take many forms, such as a signed and scanned PDF, a typed name, an email signature block, electronically clicking to confirm an agreement on a website or a signature created on-screen using a stylus or finger. The terms "secure electronic signature" or "digital signature" are often used to refer to signatures which use



encryption to confirm the authenticity of both the signature and the document to which the signature was applied. There are several software programs on the market that provide these digitally encrypted signatures, and while Canadian law has adapted to accepting electronic documents and signatures, these programs can help assuage concerns about the permanence or legitimacy of a document and its accompanying signature when a “wet” signature is not possible. A digital signature comes encrypted with information such as the date and time stamp of the signature, as well as the IP address, device, location, and name of the signer, essentially creating an electronic trail of breadcrumbs back to the original signor. These programs can also offer various levels of ID verification to ensure that the signor is in fact the person they are claiming to be, such as requiring a signor to identify themselves by uploading a photo of an ID (such as a passport or driving license) before they are granted access to the document.

### **What are the requirements for a valid electronic signature?**

Generally speaking, provincial legislation is not prescriptive in the specific requirements for an electronic signature to be valid. For example, the OECA sets out certain general and broad reliability requirements, namely that (i) the electronic signature is reliable for the purpose of identifying the person; and (ii) the association of the electronic signature with the relevant electronic document is reliable.

From a common law perspective, courts have generally found electronic signatures to be valid in a variety of circumstances, including terms of use for websites. For example, in the case of *Rudder v Microsoft Corp.*, the plaintiffs alleged, among other things, that the court should not enforce the forum selection clause in the MSN Member Agreement. This agreement was presented as part of the sign up process for the MSN service and users were required to click an “I Agree” button that was presented at the same time the terms were displayed on-screen. The plaintiffs claimed that because only a portion of the Member Agreement was displayed at a time, they did not read all the agreement and thus had no notice of the forum selection clause. The Court found that the Member Agreement was written in plain language, was not in “fine print” and the user had the opportunity to disagree and terminate the process. As such, the Court found the Membership Agreement “must be afforded the sanctity that must be given to any agreement in writing”.

Courts have even held an email signature block to be valid and binding. In *University Plumbing v Solstice Two Limited*, a series of emails were exchanged between the parties whereby the defendant acknowledged the debt owed to the plaintiff. The emails contained the defendant’s electronic signature. The court held that an email can satisfy the written acknowledgement requirements of the *Limitations Act* even though it is digitally transmitted and not signed by hand. Accordingly, the emails were held to be more than a mere acknowledgement of the debt because the communication was “repeated and fully acknowledged” and the emails contained “digital signatures”.

There are a variety of legally valid ways to execute documents when putting pen to paper for a signature is otherwise not possible. Many businesses and individuals will have to continue to adapt to these methods as most of the world continues to work remotely as a result of the COVID-19 pandemic. Organizations should be mindful of the legal requirements for different types of documents, but also be cognizant that electronic signature methods exist to ensure business can continue as usual, even if done remotely.

Content shared on Bereskin & Parr’s website is for information purposes only. It should not be taken as legal or professional advice. To obtain such advice, please contact a Bereskin & Parr LLP professional. We will be pleased to help you.