WISCONSIN BUSINESSES AND COMPLYING WITH CONSUMER DATA PROTECTION LAWS

O'NEIL CANNON
HOLLMAN DEJONG & LAING S.C.

As we have previously covered, Wisconsin businesses may be subject to the requirements of the European Union General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). Additionally, many states, including Wisconsin, and the federal government are considering similar data protection bills that may impact Wisconsin businesses. With overlapping obligations, compliance with data protection laws is an increasingly tricky business for most companies. To ensure that your company doesn't inadvertently violate any current or future laws, consider the following six steps:

Step 1: Consider the Applicability of Data Privacy Laws

Companies should determine whether existing consumer data privacy laws apply to them. The GDPR applies to companies (1) established in the EU and conducting data processing in the context of that business's activities; or (2) either: (a) offering goods or services, for free or for a fee, to individuals in the EU or (b) monitoring the behavior of individuals within the EU.

Wisconsin companies with a physical presence in the EU will almost certainly be subject to the GDPR. Without a physical presence, a Wisconsin company will nonetheless likely fall within the GDPR's scope if it offers products or services to EU individuals or businesses or if it monitors the online behavior of EU individuals or businesses.

On the other hand, the CCPA will apply to your business if it is a **for-profit business that does business in the state of California and collects** California consumers' personal information (or such information is collected on its behalf) and determines the **purposes and means** of processing California consumers' personal information, AND if it meets *one* of the following criteria:

- It has at least **$25 million** in annual gross revenues;
- It buys, sells, shares, or receives the personal information of at least **50,000 California consumers, households, or devices** per year; *or*
- It derives at least **50 percent** of its annual revenue **from selling** California consumers' personal information.

Most companies should be able to determine whether they meet the above criteria. Some businesses may struggle to determine whether or not they buy, sell, share, or receive the personal information of at least **50,000 California consumers, households, or devices** per year. Still, companies with even a small or moderate online presence will likely meet this threshold due to the broad scope of the CCPA's definition of personally identifiable information (PII).

Once you have determined that the GDPR or CCPA applies, take affirmative steps to ensure that you are in compliance.

Step 2: Map Your Company's Data

Once you have determined that the GDPR or the CCPA applies to your company, you must map the data that your company collects. Mapping will include knowing the type of data you are collecting, its source, and what happens to the data after it has been collected. You should also identify where the data is kept, what encryption or other security your company uses to protect that data, who has access to the data, and whether there are any security risks.

This step is necessary and must be taken to understand what data your company collects and where and how it is stored so that you can take appropriate steps to ensure efficient compliance with applicable data protection rules.

Step 3: Clean Up Your Company's Data

Companies should be disciplined and strict about data collection. Determine what information is necessary and what information is superfluous. Moreover, think about why certain PII is retained, rather than deleted, in view of the company's data collection goals. You may find a greater financial gain in deleting troves of PII as opposed to investing in storage and encryption. Moreover, deleting unnecessary files can help reduce the risk of inadvertently committing data protection violations.

This step will not only help ensure compliance, but it will also allow you to develop an effective and potentially financially valuable strategy for data collection.

Step 4: Create Privacy Protection Procedures and Policy

To ensure that consumers may exercise the rights to their PII granted to them under the GDPR and the CCPA, your company must have efficient processes. In crafting a privacy protection policy, consider:

- how individuals can give consent for data collection and transfer;
- the process for a consumer to request data deletion or to opt-out of data collection;
- how the company can ensure complete, effective data deletion or tagging across all

platforms;
- the process for responding to a hypothetical data breach; and
- how the company can ensure that minors give proper consent.

When creating privacy procedures and policies for your company, it is important to understand that the relevant consumer data privacy laws require transparency in matters concerning PII. Therefore, your company's privacy procedures and policies must be drafted carefully and with the complex obligations of the GDPR or the CCPA in mind.

Step 5: Update Your Company's Online Privacy Policy

Under the GDPR or the CCPA, your company must have an easily accessible and understandable privacy policy. To ensure that your company's privacy policies comply with the GDPR and the CCPA, you must ensure that it contains the following:

- A statement to residents of California or the EU that they have the right to opt-out of the sale of their data;
- An explanation that indicates how the company will inform consumers of future privacy policy updates; and
- A description of how the consumer's data will be used, including all possible uses that involve a transfer of that data.

Furthermore, you must update your company's privacy policy at least once every 12 months and notify consumers of each such update. As discussed, every privacy policy must be easily accessible and transparent. Even unintentionally complex policies may expose your company to liability.

Step 6: Update Your Company's Website

Finally, to comply with the GDPR and the CCPA, a company must include a link on its website that says "Do Not Sell My Personal Information." The link must use that specific phrasing and bring users to a page that allows them to opt-out of any sale of their data. This link must be separate from the general privacy agreement and cannot require the consumer to create a profile or account to access the opt-out. The CCPA also requires companies to create a toll-free number for consumers wanting to opt-out of the sale of their data.

After a consumer opts out, a company has two options under the CCPA: (1) it can retain the consumer's PII but exclude that PII from any sale, or (2) it can delete the consumer's data entirely. However, the GDPR requires the company to delete the consumer's data entirely. Thus, it is very important to understand whether the CCPA or GDPR (or both) applies and to have specific procedures in place to respond to a consumer's request to opt out.

What to Expect in Wisconsin

Because the GDPR and the CCPA are intentionally extraterritorial, their obligations may easily reach Wisconsin businesses. Furthermore, because of the steep fines for violating these data protection laws, Wisconsin businesses must either confirm that they are not subject to these strict requirements or take proactive steps to ensure compliance.

Even if the GDPR and the CCPA currently do not apply to your company, it may not be long until Wisconsin or the federal government implements a consumer data protection law that does. Consequently, regardless of whether you do business in the European Union or in California, beginning to implement better data collection practices now may help your companies online reputation and reduce future risks.

O'Neil, Cannon, Hollman, DeJong & Laing remains open and ready to help you.

OVERVIEW OF DATA PROTECTION LAWS IN WISCONSIN

Almost every organization in the world collects personal data from individuals, in one form or another. Indeed, most websites collect consumer information automatically. For this reason, every business must become familiar with relevant data protection laws and understand how to collect, store, use, and share data in compliance with these laws. Organizations that fail to comply with data privacy laws could incur substantial fines and other damaging consequences.

This blog post intends to give Wisconsin organizations a basic overview of consumer data privacy laws, their significance, and how such laws may apply to them.

What is Privacy Law?

"Privacy law" refers to laws governing the regulation, storage, sharing, and use of personally identifiable information, personal healthcare information, financial information, and other types of personal information. While both state and federal governments have various laws governing certain types of information privacy, as of now, no federal law exists to protect consumer data.

Given the absence of federal protection and the number of internet companies collecting—and often misusing—consumer data, several states, including Wisconsin, have developed or are beginning to develop state statutes designed to protect residents from data misuse online. Together with international data protection regulations, these state laws create an increasingly complex web of obligations for any organization collecting personal data.

What is Personally Identifiable Information?

The key to understanding and properly complying with consumer data privacy laws is understanding the term “Personally Identifiable Information” (PII). In general, PII is any information that may be used to identify an individual. Such information may include not only names, addresses, and government IDs, but also internet protocol (IP) addresses, cookie identifiers, and other automated identifiers.

Despite their many commonalities, international and domestic privacy laws have subtle differences in their categorization of PII. For example, some privacy laws allow pseudonymized or anonymized data to be excluded from PII. Pseudonymization is a reversible process that substitutes the original personal information with an alias or pseudonym such that additional information is required to re-identify the data subject. In contrast, anonymization irreversibly eliminates all ways of identifying the data subject. Similarly, IP addresses may be either static (i.e., specific to a particular computing device) or dynamic (i.e., the IP address changes over time). Static IP addresses are likely to be considered PII whereas dynamic IP addresses may not, depending on the applicable law.

An Overview of Key Data Protection Laws

Modern consumer data protection laws generally articulate both consumers’ rights to data privacy and the responsibilities of entities that collect and process personal data.

Concerning consumers, most consumer data privacy laws establish that consumers have any combination of five fundamental rights, including the right to:

- be informed that data is being collected;
- access collected data;
- rectify incorrect data;
- erase collected data; and
- object to certain uses of that data.

While these diverse privacy regimes have many similarities, they often have substantial differences, including varying definitions, scope, punishment for violations, and jurisdiction. Therefore, it’s critical to determine which laws apply to you and to thoroughly review those laws to understand your organization’s compliance obligations.

a. The European Union–General Data Protection Regulation (GDPR)

The European Union's (EU) data protection regulation, known as the GDPR, is the world's first comprehensive data protection law. Having gone into effect in 2018, the GDPR interprets PII extremely broadly and takes substantial steps to protect such PII. It covers not only IP addresses and cookies but also certain forms of pseudonymized data and metadata. The law is revolutionary in that it applies to all entities possessing or processing the personal data of EU residents, regardless of an entity's nationality. Therefore, U.S. companies who deal with EU citizens as customers, users, or clients are likely to be subject to GDPR rules and regulations.

It is crucial to determine whether your organization is subject to GDPR rules. Should EU regulators determine that a company subject to the GDPR has violated any of the GDPR articles, the company may be subject to fines for as much as €20 million or 4% of the company's global turnover, whichever is higher.

b. The California Consumer Privacy Act (CCPA)

Effective as of January 1, 2020, the CCPA is the first significant consumer data protection act in the United States. Like the GDPR, the CCPA defines PII to include any information that could, directly or indirectly, lead to the identification of any user or household.

Also similar to the GDPR, the CCPA is applied broadly to businesses globally should they do business in California. The CCPA includes specific language defining what businesses are subject to the CCPA. The CCPA applies to any for-profit business that collects, possesses, or otherwise handles the PII of California residents AND that meets any of the following criteria:

1) has annual revenues over $25 million;

2) possesses the personal information of 50,000 or more California consumers, households, or devices in any calendar year; OR

3) earns more than half of its annual revenue from selling consumers' PII.

This statute is intended to be broadly applied to commercial enterprises, regardless of geographical location and whether they explicitly target California residents. Because most businesses operate websites that automatically collect PII, such as cookies or IP addresses, even small non-California businesses risk falling under the CCPA by having a passive online presence.

The California Attorney General may fine companies up to $2,500 per non-willful violation and up to $7,500 per willful violation—amounts that add up quickly if a violation affects thousands (or millions) of users.

c. Other Relevant Consumer Data Protection Laws

Apart from California, 43 other states have made or are in the process of introducing forms of consumer data privacy bills. Wisconsin introduced three separate bills at the beginning of 2020 that would create rights and obligations concerning consumer data privacy similar to those created by the CCPA and the GDPR.

Currently, Maine and Nevada are the only two other states to have signed consumer data privacy protection bills into laws. The Maine privacy law applies only to internet service providers and not to independent businesses that may possess PII of users. The Nevada law is similar to CCPA in many ways, but it doesn't apply to non-resident companies that do not actively do business in the state.

Additionally, in March 2020 Senator Jerry Moran (R-Kan.), introduced the *Consumer Data Privacy and Security Act*; however, the federal Congress has yet to take action on the proposed bill. If passed, this federal legislation would create a clear federal standard for consumer data protection and create specific rights of consumers to access, correct, and delete personal information. The proposed bill would also create substantial obligations for businesses, including those in Wisconsin, that use, collect, or otherwise possess PII. Finally, the proposed bill would provide the Federal Trade Commission (FTC) with the specific authority to enforce these rights and obligations.

In conclusion, while there are currently no Wisconsin or federal laws directly governing the regulation, storage, sharing, and use of personally identifiable information, Wisconsin businesses could be subject to the requirements of the CCPA or the GDPR. Additionally, it seems likely that in the near future, either Wisconsin or the federal government will pass a law that directly impacts Wisconsin businesses. Moving forward, it will be very important to understand how your company's collection of personal data may be impacted.

O'Neil, Cannon, Hollman, DeJong & Laing remains open and ready to help you.

TRUMP ADMINISTRATION HALTS RESIDENTIAL EVICTIONS UNTIL DECEMBER 31, 2020

O'NEILCANNON
HOLLMAN DEJONG & LAING S.C.

Yesterday, the Trump administration announced an order temporarily halting certain residential evictions until the end of the year. The eviction moratorium, which is being enacted by the Centers for Disease Control and Prevention pursuant to its authority under Section 361 of the Public Health Service Act (42 U.S.C. § 264 *et seq.*), seeks to prevent the further spread of COVID-19. The nationwide moratorium could apply to as many as 40 million residential tenants.

Despite its reach, the moratorium is not a blanket protection for all residential tenants. To qualify for protection under the moratorium, a tenant must expect to earn no more than $99,000 this year (or no more than $198,000 if filing a joint tax return), or not have been required to report any income in 2019 to the IRS, or have received a stimulus check under the CARES Act. Further, a tenant must provide a sworn declaration to his or her landlord indicating that (1) the tenant has used best efforts to obtain government assistance, (2) the tenant is unable to pay full rent because of a loss of household income or extraordinary medical expenses, (3) the tenant is using best efforts to make partial rent payments, and (4) eviction would cause the tenant to be homeless or live with others in close quarters.

The moratorium does not relieve a tenant of his or her obligations to pay rent, and a landlord may continue to charge applicable interest, penalties, and fees under the lease for nonpayment of rent. Landlords also may still evict tenants for reasons besides not making rent, such as criminal activity, threatening the health and safety of other tenants, damaging property, and violating other provisions under the lease. Landlords who violate the order may face criminal penalties.

The order does not apply to commercial leases, nor does it apply in any state or local area that already has a moratorium on residential evictions that provides the same or greater level of protection. Nothing in the order precludes states or local authorities from imposing additional requirements.

O'Neil, Cannon, Hollman, DeJong & Laing S.C. remains open and ready to help you. For questions or further information relating to the eviction moratorium, or insolvency concerns relating to bankruptcy or receivership, please contact the authors of this article, attorneys Jessica K. Haskell and Nicholas G. Chmurski.

DON'T BE CAUGHT OFF GUARD BY THE TAX & LEGAL CONSEQUENCES OF YOUR NEW

QUARANTINE HOBBY (PART 3 OF 3)

O'NEIL CANNON
HOLLMAN DEJONG & LAING S.C.

The coronavirus pandemic has forced most of us to stay home, and as a result, we are all looking for hobbies to pick up while we are social distancing. For some, quarantine hobbies have become Netflix binge watching or mastering bread baking. For others, creative passions and hobbies such as selling handmade crafts on Etsy or unwanted junk on eBay have become sources of income. If you are dabbling in a quarantine hobby that produces income, this article describes some good business practices that are important for every business.

Be sure to also check out Part 1 of our series here, where we provide some tips for choosing between legal structures in order to better protect yourself and your business and Part 2 of our series here, where we explore the tax issues relating to your business.

Set up a separate business checking account

Opening a bank account for your business is one of the most obvious ways to show the IRS that you really are in business. Even though you might be the only person accessing funds, it is a good idea to keep your personal and business finances completely separate. Not only will this help legitimize your activity as a business, but it will be immensely helpful come tax time.

If you maintain a separate account for only business transactions, you will have a clean record of all your business expenses at the end of the year. This will prevent you from accidentally forgetting that the book of stamps you purchased was actually for home use and help you easily identify tax deductible business expenses when you are filing your taxes. If you mix personal and business finances, this process will be much more time consuming and could result in some hefty accounting fees (if you need to pay an accountant to sort it all out).

Additionally, mixing your personal and business finances could cause you to lose your business's limited liability protection. Setting up different bank accounts for your business and personal needs helps establish the business as a separate entity and protects you, as the owner, from having to satisfy business debts with your personal assets.

Obtain an EIN

A federal employer identification number (EIN) is a nine-digit number the IRS assigns to businesses for tax filing and income reporting purposes. The IRS uses the EIN to identify the taxpayer. EINs must be used by business entities—corporations, partnerships, and limited liability companies. However, most sole proprietors do not need to obtain an EIN and can use their Social Security numbers instead. Even though a sole proprietorship does not need to obtain an EIN, it may be in your best interest to obtain an EIN anyway.

There are a few good reasons to use an EIN instead of your Social Security number. First, obtaining an EIN allows you to avoid having to provide your Social Security number to clients and other members of the public. Obviously, keeping your Social Security number private limits your exposure to identity theft. Additionally, using an EIN on your tax returns and payments to others also helps to show that you're a legitimate business—in other words, this isn't just a hobby, it's separate from your personal activities. Lastly, some banks require you to have an EIN before they will set up a bank account for your business.

The good news is that obtaining an EIN is easy and free! The fastest and easiest way is to apply for an EIN is directly through the IRS website. The IRS has an online EIN Assistant tool you can use. If you are not comfortable sending information via the Internet, you can download IRS Form SS-4, *Application for Employer Identification Number*, and send it to the IRS by mail.

Maintain a good business record-keeping system

To prove to the IRS you did, indeed, make those purchases for your business, you will need a paper trail to back up your claims. Therefore, maintaining a good business record-keeping system that keeps your receipts and purchases organized is vital. Technically, if you do not have these records on file, the IRS can disallow your deduction. The IRS recommends keeping the following types of expense documents for your business:

- Account statements and invoices;
- Canceled checks;
- Credit card receipts and statements;
- Cash slips for cash payments; and
- Receipts for all entertainment, gift, transportation, and travel expenses.

The amount of time you should keep these documents varies between three years to indefinitely depending on the type of tax return you file, but the longer you keep them, the better protected you'll be if you're audited. The general rule of thumb is at least seven years—so do not immediately throw away your receipts after you have filed your taxes!

If maintaining a paper trail and a heavy file cabinet in your basement isn't your thing, an electronic record-keeping service like QuickBooks can help, since you always have a digital copy of your records available, and the calculations are always quick and accurate. Without a solid accounting software system, daily bookkeeping tasks will put a major strain on your time, and this burden will only become greater as your business grows. Regardless of the record-keeping system you choose, maintain an exhaustive record of all your finances in one place and strive to save and record receipts on at least a weekly, if not daily, basis.

Register the business with a state as a limited liability company, partnership, or corporation

Once you have chosen a legal structure for your business as detailed in Part 1 of our series, make sure you register the business with the state in which you are doing business if you chose to operate as a limited liability company (LLC), partnership, or corporation. Businesses that operate as a sole proprietorship generally are not required to register, and some states may not require registration for a small partnership either. The forms and the information required to register will differ based on the type of business being registered. But generally, the forms allow you to register a name for your business, and they also require certain information, such as the address, key officers, and the name of a contact person who will receive legal notices.

Comply with other state and federal tax laws, including collecting sales taxes and paying annual state business renewal fees or franchise taxes

***Annual statement or report*.** Many states require corporations and LLCs to submit annual reports so they can keep clear records regarding these entities. The annual report will include your entities name, your office address, and your registered agent information. The purpose of the annual report is to keep the state updated with your entities' contact information. If you fail to file your annual report, the state may automatically dissolve or shut down your business. A biennial statement may also be mandated by some states. A fee is generally required with a statement or report submission, typically ranging from $10 to over $300.

Franchise tax. Some states require corporations or LLCs to pay an annual tax to operate, which is usually called a franchise tax. The amount of the tax depends on the state collecting it and is determined through formulas based on varying criteria, such as annual revenue collection or the number of shares issued by a company.

Sales tax. You may be required to collect sales tax in your state as well. You generally collect sales tax for the state in which you conduct business on orders that are placed within or delivered to a location within that same state. So, if your studio is in Milwaukee, and you are shipping to a customer in Madison, you will be expected to collect state sales tax on that order and pay it to the state of Wisconsin. If you are shipping an order from Milwaukee to Atlanta, it is unlikely that you will need to collect state sales tax. However, for online sellers in the e-commerce space, things are a little bit murky as to where you conduct your business, so be sure to read up on tax information for your primary state of business and any others you have dealings in. Additionally, in some states you may be required to obtain a sales tax permit to collect state sales tax. You can find information about each state's sales tax permit on that state's Department of Revenue website.

Consult with Legal and Tax Professionals

Before you launch your business, you should consult with legal and tax professionals to ensure you have considered all the legal and tax requirements. Legal counsel can help explain the implications of each legal structure and other important issues beyond the scope of this series, like whether you should trademark your company name or logo, or if you need patent, copyright or intellectual property protection for any of the products you are intending to sell. Tax professionals can help explain the tax implications of forming a sole proprietorship versus a partnership or a corporation and can help you manage and file your business taxes. While your local and federal government websites are an excellent place to begin your research, it is essential to have good counsel on call to solve legal and tax issues and to provide advice before diving into the world of a small business.

The thought of running your own business may seem a bit daunting at first, but our team at O'Neil, Cannon, Hollman, DeJong & Laing S.C. is prepared and ready to help you. Please speak to your regular OCHDL contact, or the author of this article, attorney Britany E. Morrison, to get your business up and running.

DON'T BE CAUGHT OFF GUARD BY THE TAX & LEGAL CONSEQUENCES OF YOUR NEW QUARANTINE HOBBY (PART 2 OF 3)

O'NEILCANNON
HOLLMAN DEJONG & LAING S.C.

The coronavirus pandemic has forced most of us to stay home, and as a result, we are all looking for hobbies to pick up while we are social distancing. For some, quarantine hobbies have become Netflix binge watching or mastering bread baking. For others, creative passions and hobbies such as selling handmade crafts on Etsy or unwanted junk on eBay have become sources of income. If you are dabbling in a quarantine hobby that produces income, this article will address the tax-filing consequences, so they do not catch you off guard.

For helpful tips on choosing a legal structure for your business to better protect yourself and your business, check out part 1 of our series (linked here). Part 3 of our series will discuss good business practices for running your business.

Is it a Hobby or is it a Business?

The rules for how to report the income and expenses of your activity depend on whether you and the IRS classify your activity as a hobby or as a business for tax purposes. Distinguishing between a hobby and a business is not an exact science. In fact, the IRS's definition of a hobby is not entirely helpful, since it simply classifies a hobby as an activity that you engage in "for sport or recreation, not to make a profit."

Nevertheless, the IRS has provided a nonexclusive list of nine factors to be used in determining whether an activity is a legitimate business or a hobby:

1. Do you carry on the activity in a businesslike manner and maintain complete and accurate books and records?
2. Does the time and effort you put into the activity indicate an intention to make a profit?
3. Do you depend on income from the activity for your livelihood?
4. Are there losses? Are they due to circumstances beyond your control (or are they normal in the startup phase of your type of business)?
5. Have you changed your methods of operation to improve profitability?
6. Do you or your advisors have the knowledge needed to carry on the activity as a successful business?
7. Were you successful in making a profit in similar activities in the past?
8. Does the activity have the ability to make a profit in the next few years?
9. Can you expect to make a future profit from the appreciation of the assets used in the activity?

Additionally, the IRS provides a safe-harbor rule that presumes an activity to be a business versus a hobby if it has a profit in at least three of the last five years. If you have answered yes to a few of these questions or you have met the safe-harbor rule, then you most likely have a business. But if you answered no to the majority of these questions and you do not meet the safe-harbor rule, the IRS will most likely classify your activity as a hobby. The tax implications of each are explained further below.

Activity Classifies as a Hobby

If your activity is classified as a hobby, you will have to report any income you make from that hobby on your personal tax return, Form 1040, on Schedule 1, line 8, "Other Income." The income reported will be subject to income tax but not subject to self-employment tax (an additional 15.3%) as it would be if it were classified as a business.

The downside of classifying an activity as a hobby is that you cannot deduct any hobby-related expenses. Due to a change made as part of tax reform (the elimination of miscellaneous itemized deductions under the Tax Cuts and Jobs Act (TCJA)), beginning in 2018 and continuing to 2025 unless the TCJA is otherwise extended, you are no longer eligible to take a deduction for hobby expenses. This means that under the TCJA you cannot deduct any hobby expenses, but you still must report 100% of any revenue from the hobby activity as income and pay income taxes on it. And since you cannot use hobby expenses to reduce your hobby income, you will not be able to use a loss from hobby sales to reduce other income. This can be important if you make money in other activities that you intended to offset with losses.

Activity Classifies as a Business

If your activity classifies as a business or your hobby becomes a business, you are subject to a whole distinct set of tax rules. First, you will typically have to report your net income on Schedule C on your personal tax return, Form 1040. Your net income is the money you make selling your items *minus* eligible business expenses. Therefore, unlike an activity classified as a hobby, you can deduct eligible business expenses. This is a great benefit because eligible business expenses lower your taxable income, thereby lowering the amount of tax you owe as part of your tax return.

However, to be a deductible expense, a business expense must be both ordinary and necessary. An ordinary expense is one that is common and accepted in your trade or business. A necessary expense is one that is helpful and appropriate for your trade or business. Typical deductible eligible business expenses for online sellers include expenses such as:

- Fees paid to the online site/marketplace
- Cost of materials and equipment
- Shipping costs
- Bank fees
- Use of dedicated space in your home/studio for a workshop
- Legal and professional fees

To find out what deductions are available to claim and how to correctly claim those deductions, it is especially important to keep detailed records of all expenses and consult a professional, like a CPA or tax attorney. In addition, IRS Publication 535, *Business Expenses*, is a great resource that discusses common business expenses and explains what is and is not deductible.

Although you can deduct eligible business expenses if your activity classifies as a business, you could be subject to self-employment taxes. If the net income you report on your Schedule C is $400 or more, unlike an activity classified as a hobby, you will be subject to self-employment tax in addition to income tax on your activities’ earnings.

When you work as a traditional employee, your employer withholds a certain amount of money from every paycheck, which goes to pay employment taxes – 15.3% (12.4% for Social Security and 2.9% for Medicare). Half of that amount is covered by your employer, but running your own business means you are responsible for the full 15.3%, which is called the self-employment tax. You will have to manage the payment of these taxes throughout the year if you expect to pay $1,000 or more in taxes, which comes in the form of quarterly estimated tax payments. If you do not make these payments, you could be charged penalties and interest for not paying the taxes in a timely manner. For a more detailed discussion on estimated tax payments see the article here.

Despite being subject to self-employment tax, there is still a significant advantage in the fact that you can deduct eligible business expenses if your activity classifies as a business versus a hobby. However, it is important to make sure you legitimize your business in the eyes of the IRS. Part 3 of this series will focus on good business practices that are not only important for every business but help you to classify your activity as a legitimate business for tax purposes.

Bottom Line

If you are dabbling in a quarantine hobby that produces income, be sure you understand the differences between a hobby and a business for tax purposes and the tax-filing consequences of each. While declaring income earned from your hobby may seem like a hassle — especially since you cannot deduct expenses beginning in 2018 — you do not want to get in trouble with the IRS for not reporting all your income. Additionally, if the IRS decides you incorrectly classified your hobby as a business or vice versa, you could face additional taxes, penalties, and interest.

Please check back the next week for our last article in the series, which will address good business practices for operating and running an online business. And, If you are interested in learning more about the differences between a hobby and a business for tax purposes and how it might affect your tax filing requirements, or how to incorporate or organize a business entity, please contact the author of this article attorney Britany E. Morrison at O'Neil, Cannon, Hollman, DeJong & Laing S.C. to discuss how we are able to assist you.

DON'T BE CAUGHT OFF GUARD BY THE TAX & LEGAL CONSEQUENCES OF YOUR NEW

QUARANTINE HOBBY (PART 1 OF 3)

The coronavirus pandemic has forced most of us to stay home, and as a result, we are all looking for hobbies to pick up while we are social distancing. For some, quarantine hobbies have become Netflix binge watching or mastering bread baking. For others, creative passions and hobbies such as selling handmade crafts on Etsy or unwanted junk on eBay have become sources of income. If you are dabbling in a quarantine hobby that produces income, here are some tips for choosing between legal structures in order to better protect yourself and your business.

Whether you have just started selling your handmade crafts online, or you are a veteran in the trade, one of the most important legal questions for online sellers to determine is: **What is the best legal structure for my business?** This article will help you decide on the best way to structure your newly founded business.

Please check back in the next two weeks for our other articles, which will address tax issues relating to your online business, and good business practices for operating and running an online business.

Remember, your online business is a *business* whether you like it or not, so please think about the appropriate business structure

Your online business is your business, and it is important that you set up your business as a legal business entity. There are a number of legal business structures to choose from. Which business structure you choose will impact the taxes you pay, the paperwork you are required to file in order to establish your business, and whether you can be held personally liable if someone sues your business. The most common legal structures are as follows and will be described in detail below:

- Sole proprietorship
- Limited liability company
- Corporation

Easy as 1, 2, 3: Sole Proprietorships

A sole proprietorship is an unincorporated entity, which is the easiest and cheapest way to operate your business; however, it comes with more risks than a limited liability company or corporation. With a sole proprietorship, you don't need to file any legal forms with the state you are operating in or pay any fees to the state to establish your sole proprietorship. If you have already sold one handmade craft, you're technically operating a sole proprietorship and no legal paperwork is needed to be filed. That was easy, right?

If you are operating as a sole proprietorship but would prefer to operate under a different name other than your own, you may need to file a certificate with your state for a "DBA" or "doing business as" name. For example, if your name is Bob Smith then technically your sole proprietorship is also named Bob Smith. However, if Bob sells handmade fishing poles on his online shop, he can choose to do business as "Bob's Fantastic Fishing Poles" or any other name he chooses to do business as.

Further, depending on what you're selling and where you're selling from, you may also need to obtain certain business licenses (e.g., a seller's permit). Therefore, before you start selling, it's important to look up and comply with local and state laws to avoid violations and fines.

One of the major drawbacks with operating a business as a sole proprietorship is the fact that you may face personal liability if someone is harmed or injured by your handmade crafts and you end up being sued. Not only are you risking your online business's livelihood, you could also be risking your home, your car, the money in your bank account, and more. All those things might not be worth risking for a few hundred dollars in your pocket, right? If you are selling handmade crafts that come with even a slight risk of being injurious, toxic, or harmful to individuals, we highly recommend that you consider incorporating or organizing your business through a corporation or limited liability company, which is described in more detail below.

Uncharted Waters: Limited Liability Companies and Corporations

Whether you have quit your day job to make custom wooden tables or are merely crafting and selling earrings out of your basement as a hobby, it is still a good idea to form a limited liability company or corporation to protect yourself from personal liability (as described above).

Although forming a limited liability company or incorporating your business will be more expensive and time consuming than starting a sole proprietorship, the time and money will likely be worth it. In order to form a limited liability company or corporation you will need to pay fees and file paperwork with the Secretary of State (or similar office) in the state in which you intend to organize your limited liability company or incorporate your business. Depending on your needs and wants, it may make sense to research certain state laws to determine whether your home state or another state is best for formation of your new business.

A limited liability company and a corporation will both limit your personal liability to how much you put into the company. This means that if someone is to get injured from one of your business's handmade crafts, theoretically (if all corporate and limited liability procedures are followed) the most you could end up losing is the assets, including cash, that you have in the company. While this may not be an ideal situation, it is much better than losing your personal assets over a $10 set of earrings that harms an individual.

Lastly, the process of incorporation typically requires more time and money than other legal entities. Not only does a corporation require a board of directors and more formal requirements than that of a limited liability company (like holding regular board meetings and recording minutes), a corporation is taxed differently than a limited liability company, which could be a deciding factor on how you structure your newly founded online business.

The thought of incorporating or organizing a business entity may seem a bit daunting at first, but our team at O'Neil, Cannon, Hollman, DeJong & Laing S.C. is prepared and ready to help you. Please speak to your regular OCHDL contact, or the authors of this article, attorney Britany E. Morrison, to get your business up and running.

COVID-19 RAISES PRIVACY ISSUES FOR MAJOR-LEAGUE BASEBALL

O'NEILCANNON
HOLLMAN DEJONG & LAING S.C.

After months of delay trying to address COVID-19 issues, the 2020 Major League Baseball ("MLB") season finally opened Thursday night with the New York Yankees defeating the Washington Nationals, 4-1, and the Los Angeles Dodgers pulling away from the San Francisco Giants for an 8-1 victory. Because of the COVID-19 pandemic, this season – assuming it is not called off because of COVID-19 outbreaks – will be unlike any prior MLB season. The regular season has been reduced from 162 games to 60 games, the number of playoff teams was expanded from 10 to 16 teams, games are being played in empty stadiums, and players, coaches, and other staff are subject to extensive COVID-19 testing and daily monitoring.

As of July 17, 80 players have tested positive for COVID-19, 17 of which tested positive after teams began their workouts on July 1. Of those 80 players, the general public knows the identity of only 56 of them. Why only 56, especially since MLB clubs traditionally have disclosed details of a player's injury? For example, when New York Mets pitcher Noah

Syndergaard tore the ulnar collateral ligament in his pitching elbow in March, the Mets announced that Syndergaard had suffered the injury and would undergo Tommy John surgery. The Mets later announced that the surgery had been successful, and that Syndergaard was expected to pitch again at some point during the 2021 season.

MLB clubs are more tight-lipped about COVID-19 issues. MLB has effectively created a COVID-19 Related Injured List for players who have tested positive, have been exposed, or have shown symptoms of the COVID-19. The list does not differentiate between players who have tested positive and players who have been exposed to someone who has tested positive for COVID-19, and is not being published as a stand-alone list. Instead, players with positive COVID-19 testing or exposure status will be acknowledged on the normal injury report just like any other injured player. Their injury, however, will be described as an undisclosed injury, an illness, or a non-baseball injury. While naming a player to the injury list with a designation of "undisclosed" does open the door for public speculation regarding a player's health status, the various designations on the list do not function to definitively confirm that a particular player has tested positive for or been exposed to the virus that causes COVID-19.

Why do MLB clubs disclose less about the status of a player who is missing games because of COVID-19 than a player one who is out for the season with a torn elbow ligament?

The simple answer is that the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Americans with Disabilities Act ("ADA") provide broad health privacy and confidentiality protections for players. Specifically, HIPAA and the ADA each restrict the clubs' ability to publicize information about employee illness without permission.

How do HIPAA and the ADA Apply?

HIPAA applies to an MLB club in its role as a health-care provider to the players. HIPAA is a federal law that was created to protect sensitive patient health information and prevents disclosure of individual health information without such individual's consent. This privacy rule generally applies only to specified types of covered entities and their associates. Covered entities include healthcare providers and group health insurance plans. Certain business associates and vendors of a covered entity can also be required to observe HIPAA's requirements. Where an entity is either not regulated by HIPAA, or is subject to HIPAA, but has obtained individual consent, the federal privacy law does not prevent the disclosure of personal medical information. Because professional sports teams provide healthcare to their players via team doctors, they are healthcare providers under HIPAA. The terms and conditions of professional athletes' employment, as documented in the applicable collective bargaining agreement, generally requires player consent to disclose individual medical information relevant to team status.

The ADA applies to an MLB club in its role as an employer. The ADA functions to prohibit employers from discrimination against employees on the basis of a disability and to require employers to treat all information about employee illness as a confidential medical record. While federal guidance indicates that COVID-19 status is unlikely to constitute a disability, the Equal Employment Opportunity Commission ("EEOC") has made clear that employers must treat employee COVID-19 status as confidential.

Why is There Different Treatment?

An elbow injury and a positive COVID-19 test are treated differently because of HIPAA, the ADA, and MLB's collective bargaining agreement and standard player contract. MLB players and clubs must operate in accordance with the health information disclosure rules as currently codified under Article XIII.G.(1) of the collective bargaining agreement known as the 2017-2021 Basic Agreement (the "CBA") and by Paragraph 6(b)(1) of each standard player contract, known as the Uniform Player's Contract ("UPC"). Under these agreements, each player is required to execute a HIPAA-compliant authorization for the use and disclosure of health information about the player. By signing the UPC, the player authorizes disclosure of employment-related injuries. The UPC incorporates the relevant health information disclosure provisions of Article XIII.G. of the CBA, Section 4, which provide that:

> [for] public relations purposes, a Club may disclose the following general information about employment-related injuries: (a) the nature of a Player's injury, (b) the prognosis and the anticipated length of recovery from the injury, and (c) the treatment and surgical procedures undertaken or anticipated in regard to the injury.

If a medical condition, other than an employment-related injury, prevents a player from playing and the player has not provided the club with specific written authorization to disclose information about the medical condition, the club may disclose only that a medical condition is preventing the player from playing and the anticipated absence of the player from the club. COVID-19 status, therefore, is not deemed to be an employment-related injury that would allow an MLB club to disclose details regarding prognosis and treatment. Although a player may authorize a team to disclose his COVID-19 status, such authority is not automatic under either HIPAA or the documents governing the employment relationship. The ADA does not explicitly address employee authorization of an employer to disclose medical information, but does permit limited disclosure as necessary to respond to a request for reasonable accommodation.

In practical terms, this compliance with the HIPAA privacy and ADA confidentiality rules with respect to COVID-19 means that even if a player tests positive, the club or its staff may not disclose that to the public unless granted permission to do so by the player. Any unauthorized disclosure could constitute a HIPAA violation, for which significant federal civil monetary penalties may apply if the U.S. Department of Health and Human Services investigates a compliant or performs a compliance audit. Additionally, a player might be able to bring a collective bargaining grievance, or to allege a breach of the employment contract.

Lessons for the Rest of Us

Of course, most businesses are not professional sports franchises with collective bargaining agreements providing HIPAA disclosure consent. The caution displayed by the MLB in avoiding the disclosure of player COVID-19 status, however, is a reminder to all employers with access to employee health information and records to carefully assess which health-related information disclosures may or may not be permitted under applicable law.

HIPAA

HIPAA is a complex health privacy law with multiple exceptions and with sometimes conflicting state law counterparts. Health care providers, employer sponsors of self-insured group health plans and their business associates are subject to its requirements and should take care to ensure that affirmative compliance actions are taken and maintained. Violations of these rules, as well as the inability to demonstrate operational and documented (written) compliance, can subject the health care providers, health plan sponsors, or their associates, to large civil, or even criminal, penalties.

The ADA, FMLA, and GINA

For employers who, unlike MLB clubs, are not directly subject to HIPAA, it is important to remember that other laws provide separate protections for employee health information. Any information known to an employer regarding an employee's disability or gathered as a result of an employer-provided medical examination (which can include taking a temperature) should remain confidential. Employers must maintain all information about employee illness as a confidential medical record in compliance with the ADA and EEOC guidance. Similarly, employers subject to the Family and Medical Leave Act ("FMLA") or the Emergency Family Medical Leave ("EMFL") provisions of the CARES Act must confidentially maintain any records and documents relating to employee (and family) medical certifications and medical histories and created for FMLA or EMFL purposes. The Genetic Information Nondisclosure Act ("GINA") also requires employers to keep all genetic information, including information about an individual's genetic tests, the genetic tests of a family member, family medical history, regarding employees confidential. The ADA, FMLA, EFML, and GINA all require that such records be stored separately from the usual personnel files.

If you have questions related to your business's obligations under the ADA, FMLA, CARES Act, or GINA, or HIPAA, or seek attorney-client privileged review of your current compliance program, including as to HIPAA policies and procedures, please contact your regular OCHDL attorney or Pete Faust.

NEW ACT PROVIDES MORE FLEXIBILITY TO PPP BORROWERS

Today President Trump signed the Paycheck Protection Program Flexibility Act of 2020 (the "Act") to amend certain provisions of the CARES Act related to the forgiveness of loans under the Paycheck Protection Program ("PPP") and for a number of other purposes.

Here are some of the key takeaways:

- **Deadline to Use the Loan Proceeds**: Borrowers can now use their PPP loan over a period of 24 weeks, tripling the current covered period of eight weeks.[1]
- **Forgivable Uses of the Loan Proceeds**: Borrowers must use at least 60% of their PPP loan on payroll costs, amending the previous rule that required borrowers to use 75% of their PPP loan for payroll costs. The remaining 40% may be used for allowable non-payroll expenses.
- **Extension of Time for Rehiring Workers**: The period to rehire employees has been extended from June 30, 2020 to December 31, 2020.
- **New Exemptions from Rehiring Workers**: Two exemptions were added to the PPP's loan forgiveness reduction penalties.

    1. The forgiveness amount will not be reduced due to a reduced full time employee count if the borrower can document that it attempted, but was unable, to rehire individuals who had been employees on February 15, 2020.
    2. The forgiveness will not be reduced due to a reduced full time employee count if the borrower, in good faith, can document an inability to return to the "same level of business activity" as prior to February 15, 2020 due to sanitation, social distancing, and worker or customer safety requirements.

- **Payroll Tax Deferral**: The payroll tax deferral is now available to a borrower that has its loan forgiven. Previously, the deferral was available only to borrowers that did not have their loan forgiven.
- **Loan Deferral Period**: The loan deferral period has been changed to (i) whenever the amount of loan forgiveness is remitted to the lender, or (ii) 10 months after the applicable forgiveness covered period if a borrower does not apply for forgiveness during that 10 month period. Previously, a borrower's deferral period was to be

between six and 12 months.
- **Loan Maturity Date**: The maturity date for the payment of the unforgiven portion of the PPP loan has been extended from two years to five years.[2]

Borrowers are now able to spend their PPP loan proceeds in a more flexible manner than previously permitted. As with the initial rollout of the PPP, it will be up to the Department of the Treasury and the Small Business Administration to provide regulations with respect to the Act.

O'Neil, Cannon, Hollman, DeJong & Laing remains open and ready to help you. For questions or further information relating to the Paycheck Protection Program, please speak to your regular OCHDL contact, or the authors of this article, attorneys Jason Scoby and Pete Faust.

[1] If the borrower would like, it can still elect to have the eight week period apply.

[2] This provision of the Act only affects borrowers whose PPP loan is disbursed after its enactment. With respect to an already existing PPP loan, the Act states specifically that nothing in the Act will "prohibit lenders and borrowers from mutually agreeing to modify the maturity terms of a covered loan."

SBA PUBLISHES PPP LOAN FORGIVENESS APPLICATION

O'NEILCANNON
HOLLMAN DEJONG & LAING S.C.

On Friday, the SBA published its Paycheck Protection Program Loan Forgiveness Application, which includes instructions for completing the application. The application can be found here. Of note, the application contains further information with respect to the timing of paying and incurring payroll costs as that relates to calculating the amount eligible for forgiveness. Additionally, the application provides certain borrowers (those with biweekly or more frequent payroll periods) flexibility in terms of when the eight-week "covered period" begins.

O'Neil, Cannon, Hollman, DeJong & Laing remains open and ready to help you. For questions or further information relating to the Paycheck Protection Program, please speak to your regular OCHDL contact, or the authors of this article, attorneys Jason Scoby and Pete Faust.

SBA ISSUES FURTHER GUIDANCE ON PPP LOAN REPAYMENT SAFE HARBOR; ALL LOANS UNDER $2 MILLION DEEMED TO HAVE BEEN RECEIVED IN GOOD FAITH

O'NEIL CANNON
HOLLMAN DEJONG & LAING S.C.

This morning, the SBA issued much anticipated additional guidance with respect to the Paycheck Protection Program's repayment safe harbor. The new guidance provides significant clarity with respect to how the SBA will evaluate whether a borrower made the following certification in good faith when submitting its loan application:

"Current economic uncertainty makes this loan request necessary to support the ongoing operations of the Applicant."

With the new guidance, the SBA makes clear that all borrowers receiving a loan of less than $2 million will be deemed to have made the certification in good faith. Loans to borrowers and their affiliates will be combined for purposes of calculating this $2 million threshold.

Moreover, borrowers (including their affiliates) receiving more than $2 million will still have the opportunity to demonstrate that they made the certification in good faith, and if the SBA determines that they are not able to do so, the SBA will then permit those borrowers to repay the loan without any further penalties.

The SBA's FAQ #46 states in full:

46. Question: How will SBA review borrowers' required good-faith certification concerning the necessity of their loan request?

Answer: When submitting a PPP application, all borrowers must certify in good faith that "[c]urrent economic uncertainty makes this loan request necessary to support the ongoing operations of the Applicant." SBA, in consultation with the Department of the Treasury, has determined that the following safe harbor will apply to SBA's review of PPP loans with respect to this issue: Any borrower that, together with its affiliates, received PPP loans with an original principal amount of less than $2 million will be deemed to have made the required certification concerning the necessity of the loan request in good faith.

SBA has determined that this safe harbor is appropriate because borrowers with loans below this threshold are generally less likely to have had access to adequate sources of liquidity in the current economic environment than borrowers that obtained larger loans. This safe harbor will also promote economic certainty as PPP borrowers with more limited resources endeavor to retain and rehire employees. In addition, given the large volume of PPP loans, this approach will enable SBA to conserve its finite audit resources and focus its reviews on larger loans, where the compliance effort may yield higher returns.

Importantly, borrowers with loans greater than $2 million that do not satisfy this safe harbor may still have an adequate basis for making the required good-faith certification, based on their individual circumstances in light of the language of the certification and SBA guidance. SBA has previously stated that all PPP loans in excess of $2 million, and other PPP loans as appropriate, will be subject to review by SBA for compliance with program requirements set forth in the PPP Interim Final Rules and in the Borrower Application Form. If SBA determines in the course of its review that a borrower lacked an adequate basis for the required certification concerning the necessity of the loan request, SBA will seek repayment of the outstanding PPP loan balance and will inform the lender that the borrower is not eligible for loan forgiveness. If the borrower repays the loan after receiving notification from SBA, SBA will not pursue administrative enforcement or referrals to other agencies based on its determination with respect to the certification concerning necessity of the loan request. SBA's determination concerning the certification regarding the necessity of the loan request will not affect SBA's loan guarantee.

O'Neil, Cannon, Hollman, DeJong & Laing remains open and ready to help you. For questions or further information relating to the Paycheck Protection Program, please speak to your regular OCHDL contact, or the authors of this article, attorneys Jason Scoby and Pete Faust.